ENCRYPT 4.0

Gemeinsame Initiative zur Entwicklung von Cyber-Arbeitskräften, die es der europäischen Industrie ermöglichen soll, den Mangel an Fachkräften für Cybersicherheit zu überwinden,

Nr. 2020-1-RO01-KA202-079983

O3: Dokumentarische Sammlung von Cyber-Attacken

Co-funded by the Erasmus+ Programme of the European Union

Die Unterstützung der Europäischen Kommission für die Erstellung dieser Veröffentlichung stellt keine Billigung des Inhalts dar, der ausschließlich die Meinung der Autoren widerspiegelt, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden.

INHALTE

EINLEITUNG

Mit dem Aufkommen der IT und der vierten industriellen Revolution stehen die Unternehmen vor neuen Herausforderungen in Bezug auf Cybersicherheit und Datenschutz. Dies gilt insbesondere für KMU`s in der Produktion, die häufig nicht über die internen Ressourcen und Kapazitäten verfügen, um die mit den neu eingeführten Industrie-4.0-Technologien verbundenen Cybersicherheitsrisiken wirksam zu bewerten. Gleichzeitig werden KMU`s immer häufiger Opfer verschiedener Cyberkriminalität. Laut dem jüngsten Verizon 2021 Data Breach Investigations Report (Verizon, 2021) sind KMU`s Opfer von Cyberangriffen und im Vergleich zu großen Unternehmen viel anfälliger dafür, da es ihnen an Ressourcen, Mitarbeitern, Informationen und allgemeinen Kapazitäten fehlt, um die Risiken eines Cyberangriffs abzuwehren.

Inzwischen haben Cyber-Bedrohungen unterschiedliche Quellen und werden immer raffinierter. Wenn die Teams zum Beispiel keine Erfahrung mit ähnlichen Schwachstellen haben und keine klare Anleitung haben, wie sie darauf reagieren sollen, kann es Tage oder sogar Wochen dauern, bis sie richtig reagieren, was für einige Produktionsprozesse fatal sein kann. Laut dem KMU-IT-Sicherheitsbericht 2021 gelten Mitarbeiter, die sich nicht an Richtlinien halten, als größtes Hindernis für die Cybersicherheit, und diese Tendenz hat sich mit der Zunahme des Homeoffice aufgrund der COVID-19-Pandemie noch verschärft (Untangle, 2021). Ein Verstoß gegen die Cybersicherheit hat jedoch nicht nur Auswirkungen auf Menschen, sondern kann auch zu finanziellen Verlusten, zum Verlust des Vertrauens der Kunden und zu einem beschädigten Ruf führen (Acronis, 2021).

Vor diesem Hintergrund hat das Encrypt 4.0-Konsortium dieses Dokument entwickelt, das als Know-how-Tool dienen soll. Es bietet Zugang zu kritischen Analysen realer Cyberangriffe und zu den daraus gezogenen Lehren sowie zu Fahrplänen, wie diese verhindert, identifiziert, bekämpft und wiederhergestellt werden können.

Die Encrypt 4.0-Dokumentenbatterie zu Cyberangriffen ist speziell auf die Bedürfnisse von KMU des verarbeitenden Gewerbes in der EU zugeschnitten, die im Kontext von Industrie 4.0 tätig sind, und stellt eine Zusammenstellung von Fallstudien zu Cyberangriffen dar, die darauf abzielt, KMU`s bei der Verbesserung ihrer Cybersicherheit und der Verhinderung von Cyberangriffen zu unterstützen.

STRUKTUR & METHODE

Die Encrypt 4.0-Dokumentensammlung enthält insgesamt 18 Fallstudien. Jeder der ENCRYPT 4.0-Partner hat drei Fallstudien zu realen Cyberangriffen entwickelt, die auf Desk Reserach, persönlichen Erfahrungen und Beobachtungen sowie ausführlichen Interviews mit Geschäftsführern, Cybersicherheitsexperten und IT-Fachleuten beruhen und verschiedene Arten von Cyberangriffen abdecken und eine kritische Analyse der Gründe für die Sicherheitsverletzungen, die Art und Weise, wie sie angegangen wurden, und die Folgen liefern.

Das ENCRYPT 4.0-Konsortium hat ein spezielles Modell "PREVENT-IDENTIFY-RESPOND-RECOVER" (PIRR) entwickelt, das auf dem Modell "Identify, Protect, Detect, Respond and Recover" des National Institute of Standards and Technology (NIST) basiert. Die Art der Cyber-Attacken basiert auf dem STRIDE-Modell sowie dem MITRE ATT&CK-Framework. Die Analyse des PIRR-Modells enthält 4 Hauptkategorien/Abschnitte, die auf den wichtigsten Schritten zur Bekämpfung eines

Cybersicherheitsproblems basieren, sowie Abschnitte, in denen Lehren gezogen werden (siehe Abb. 1).

Abb. 1. Kategorien des Modells "Vorbeugen - Erkennen - Reagieren - Wiederherstellen" (PIRR)

VORBEUGEN

Abschnitt befasst sich mit der Verringerung des Risikos von Cyberangriffen und Präventivmaßnahmen und umfasst für jede Fallstudie Folgendes:

Spezifische Sicherheitspraktiken, die sich bei realen Cyberangriffen bewährt haben;

Falsche Vorstellungen von Cybersicherheit: Praktiken, die jedes Unternehmen anwandte und die bei tatsächlichen Vorfällen keine oder sogar negative Auswirkungen hatten.

ERKENNEN

Das Hauptziel dieses Abschnitts besteht darin, KMU dabei zu helfen, zwischen den verschiedenen Arten von Cyberangriffen zu unterscheiden, die anhand des STRIDE-Modells und des MITRE ATT&CK-Frameworks kategorisiert werden. Das STRIDE-Modell ist ein systemorientiertes Bedrohungsmodell auf hoher Ebene, das sich auf die Identifizierung allgemeiner Kategorien von Angriffen konzentriert. Es umfasst die folgenden 6 Kategorien:

+Spoofing

+Manipulation

+Ungültigkeitserklärung

+Offenlegung von Informationen

+Verweigerung des Dienstes

+Aushebelung von Privilegien

Für die Fallstudien zu ENCRYPT 4.0 wurde STRIDE verwendet, um die Bedrohungen auf einer höheren Ebene zu identifizieren, während das MITRE ATT&CK-Framework eingesetzt wurde, um die Angriffe detaillierter zu beschreiben. Das ATT&CK-Framework geht bewusst von der Sichtweise des Angreifers aus, um Unternehmen dabei zu helfen, zu verstehen, wie Angreifer vorgehen, sich vorbereiten und Angriffe erfolgreich durchführen.

REAGIEREN

In diesem Abschnitt werden Situationen dargestellt, in denen die Bedrohung bereits vorhanden ist. Er enthält eine Analyse realer Cyberangriffe und Ratschläge, wie man in ähnlichen Fällen reagieren sollte, nachdem man sie erkannt hat.

Die Cyberangriffe in den Fallstudien werden in folgendem Format skizziert:

WER: der Angreifer

WER: die Zielorganisation

WARUM: die Motive für den Angriff (war er zufällig oder gezielt)

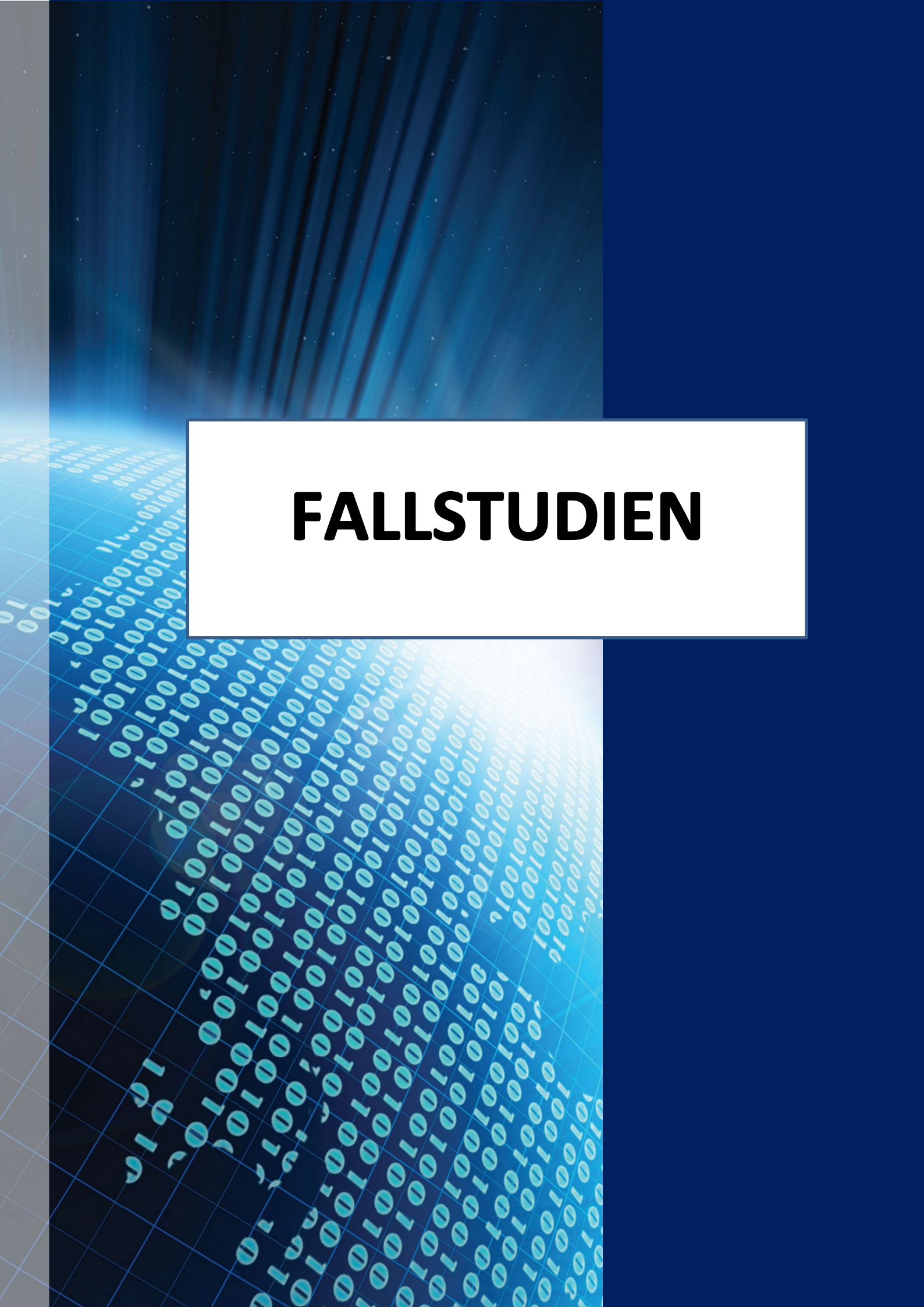
WAS: das Zielobjekt

WIE: Beschreibung des Angriffs und der verwendeten Techniken.

STRATEGIE: Wie wurde die Bedrohung bekämpft und welche Maßnahmen hatten keine oder negative Auswirkungen?

WIEDERHERSTELLEN

Dieser Abschnitt enthält Informationen über die Folgen des Angriffs sowie eine Analyse darüber, wie das System wiederhergestellt werden kann, nachdem einige Prozesse beschädigt wurden, und wie der Zugang zu den verlorenen Daten wiederhergestellt werden kann, basierend auf den im Abschnitt RESPOND beschriebenen realen Angriffsfällen. Der Abschnitt folgt den STRIDE & MITRE ATT&CK-Modellen, die Wiederherstellungspraktiken auf der Grundlage jeder spezifizierten Gruppe von Cyber-Bedrohungen skizzieren, die im Abschnitt IDENTIFY vorgestellt wurden.


FALLSTUDIEN

FALLSTUDIE 1: REVERSE SHELL

BETROFFENE ORGANISATION

Innovalia Association ist ein privates und unabhängiges Technologiezentrum, das von der Innovalia-Gruppe gegründet wurde, um eine kritische Masse zu bilden, die in der Lage ist, ihre langfristigen Forschungsambitionen und strategischen Ziele erfolgreich zu verwirklichen. Innovalia ist eine Allianz für technologieorientierte KMU mit Sitz in Spanien. Sie verfügt über eine internationale Präsenz mit Büros im Baskenland, in Madrid, Katalonien, auf den Kanarischen Inseln, in Europa, Asien, im Nahen Osten sowie in Mittel- und Südamerika. Seit ihrer Gründung hat die Innovalia Association ein besonderes Gespür für die Besonderheiten technologiebasierter KMU entwickelt und ein Bewusstsein für diese entwickelt. Heute ist sie führend im Bereich der Forschung und Entwicklung von und für KMU`s in Spanien. Außerdem bietet sie Lösungen zur Erleichterung internationaler Innovationsprozesse für KMU`s an. Als technologischer Akteur des Technologie-Netzwerks des Baskenlandes (Innobasque) bündelt Innovalia die Kompetenzen, Labors und Ressourcen der Unternehmen, die den Verband gegründet haben

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Informationen für diese Fallstudie wurden durch ein ausführliches Interview mit einem IT-Techniker des Unternehmens gesammelt. Während des Gesprächs stellte der Interviewer erste Fragen, um den Befragten zu ermutigen, zu antworten. Die fehlenden Informationen wurden im Nachhinein mit den von der befragten Person bereitgestellten Daten ergänzt.

VORBEUGEN

Die von Innovalia vor dem Vorfall angewandte Praxis war die Installation einer **Firewall-Software.**

Spezielle Sicherheitspraktiken

- ☑ **die Sensibilisierung der Mitarbeiter für nicht vertrauenswürdige Mails.** In diesem Fall schickte ein Hacker eine scheinbar legitime E-Mail, in der er unsere Mitarbeiter aufforderte, auf einen Link in der E-Mail zu klicken, um das Zugangspasswort zurückzusetzen, unter dem Vorwand, dass mehrere erfolglose Anmeldeversuche registriert worden waren.
- ☑ **die Installation interner Firewalls zur Verstärkung ihrer externen Standard-Firewall.** Als die Mitarbeiter während der COVID-19-Pandemie von zu Hause aus arbeiteten, mussten sie eine Firewall in ihrem Heimnetzwerk installieren.

"Command Injection ist ein Cyberangriff, bei dem ein Angreifer die Kontrolle über das Host-Betriebssystem übernimmt, indem er über einen Befehl Code in eine anfällige Anwendung einschleust. Dieser Code wird unabhängig von allen Sicherheitsmechanismen ausgeführt und kann dazu verwendet werden, Daten zu stehlen, Systeme zum Absturz zu bringen, Datenbanken zu beschädigen und sogar Malware zu installieren, die später verwendet werden kann. (StackHawn, 2022)

ERKENNEN

Die Art und Weise des Cyberangriffs war: **Code-Injektionen in eine Schwachstelle im Apache-Webserver des Unternehmens durch Remote-Befehlsausführung.** Diese Art des Angriffs kann gemäß dem MITRE ATT&CK-Framework detailliert, wie unten dargestellt, beschrieben werden:

Aktives Scannen: Scannen von IP-Blöcken und Schwachstellen-Scanning

- ☑ Erster Zugang: Externe Ferndienste
- ☑ Ausführen: Befehls- und Skripting-Interpreter: Power Shell
- ☑ Privilege Escalation
- ☑ Process Injection: njektion von Dynamic-Link-Bibliotheken; Injektion von portablen ausführbaren Dateien; Thread Execution Hijacking; Asynchronous Procedure Call; Thread Local Storage; Ptrace System Calls; Proc Memory; Extra Window Memory Injection;
- ☑ Ereignisausgelöste Ausführung: Änderung der Unix-Shell-Konfiguration,
- ☑ Umgehung der Verteidigung: Prozess- und Vorlageninjektion
- ☑ Exfiltration: Transfer Data to Cloud Account.
- ☑ Auswirkung:
  - Datenmanipulation: Gespeicherte, übertragene und Laufzeitdatenmanipulation
  - Dienst anhalten
  - System herunterfahren/neustarten

REAGIEREN

- ☑ **WO:**. Der Angreifer konnte nicht genau identifiziert werden. Nur der Herkunftsort, China, war bekannt.
- ☑ **Wem:** Innovalia Association
- ☑ **Warum:** Es war random
- ☑ **Was:** System der Organisation Innovalia
- ☑ **Wie:** Prozessinjektion mit Remote-Befehlsausführung.
- ☑ **STRATEGIE:** Die Bedrohung wurde mit der Firewall bekämpft, die zu diesem Zeitpunkt auf dem Server installiert war. Befolgen Sie die im folgenden Abschnitt beschriebenen Schritte, um IPs zu blockieren

WIEDERHERSTELLEN

Die wichtigsten Folgen des Angriffs waren:

- ☑ Gefährdung des Systems
- ☑ Forschung und Analyse
- ☑ Update der Server Versionen
- ☑ Anmeldeinformationen ändern

Die **Wiederherstellungsstrategi**e konzentrierte sich auf das Blockieren der IP-Adresse durch die Firewall:

Melden Sie sich zunächst bei dem Server an, auf dem Sie die IP-Adresse blockieren möchten. Klicken Sie dann auf Start, geben Sie Windows-Firewall mit erweiterter Sicherheit ein, und drücken Sie die Eingabetaste. Klicken Sie im linken Fensterbereich auf Eingehende Regeln, um die aktuell konfigurierten Regeln im mittleren Fensterbereich anzuzeigen.

Klicken Sie im rechten Fensterbereich auf Aktionen > Neue Regel: Wählen Sie für Regeltyp die Option Benutzerdefiniert und klicken Sie auf Weiter; wählen Sie für Programm die Option Alle Programme und klicken Sie auf Weiter; wählen Sie für Protokoll und Ports die Option Beliebig aus der Dropdown-Liste Protokolltyp und klicken Sie auf Weiter; und wählen Sie für Geltungsbereich: unter Für welche entfernten IP-Adressen gilt diese Regel? die radiale Option: Diese IP-Adressen: Klicken Sie auf Hinzufügen.

Geben Sie dann die IP-Adresse ein, die Sie für den Server sperren möchten, und klicken Sie auf OK. Sie können auch einen Bereich von IP-Adressen blockieren, indem Sie die radiale Option Dieser IP-Adressbereich: auswählen. Nachdem Sie die IP-Adressen hinzugefügt haben, klicken Sie auf Weiter. Wählen Sie unter Aktion die Option Verbindung blockieren und klicken Sie auf Weiter. Lassen Sie bei Profil alle Optionen aktiviert und klicken Sie auf Weiter. Geben Sie der Regel unter Name einen beschreibenden Namen, z. B. Blacklisted IPs. Sie können auch eine optionale Beschreibung der Regel eingeben. Klicken Sie auf Fertig stellen. Die neu erstellte Regel mit dem angegebenen Namen wird nun im mittleren Fensterbereich Eingehende Regeln angezeigt. Um die Regeln alphabetisch nach Namen zu ordnen, können Sie auf die Spaltenüberschrift Name klicken. Wenn Sie die Regel deaktivieren müssen, klicken Sie mit der rechten Maustaste auf die Regel in der Liste und klicken Sie auf Regel deaktivieren. Wenn Sie den Bereich der IP-Adressen für die Regel ändern müssen, klicken Sie mit der rechten Maustaste auf die Regel in der Liste und dann auf Eigenschaften. Klicken Sie dann auf die Registerkarte Bereich, nehmen Sie die erforderlichen Änderungen vor, und klicken Sie auf Übernehmen.

LESSONS LEARNT

Wir haben gelernt, dass es besser ist, bestimmte präventive und defensive Maßnahmen zu ergreifen, die für diese Art von Angriffen nützlich sind, wie z. B.:

- ☑ den Server auf dem neuesten Stand zu halten
- ☑ fügen Sie dem Server-Rechner eine Überwachung hinzu
- ☑ das Netz in VLANS zu segmentieren und
- ☑ die Isolierung von Maschinen, die der Außenwelt ausgesetzt sind.

FALLSTUDIE 2: DIE LEICHTFERTIGKEIT EINES MITARBEITERS

BETROFFENE ORGANISATION

Die Organisation setzt ein Intrusion Detection System (IDS) ein, das das CARSA-Netz auf böswillige Aktivitäten oder Richtlinienverstöße überwacht. CARSA setzt Firewall-Software ein, um ihr Netzwerk und System vor unbefugtem Zugriff zu schützen.

Spezifische Sicherheitspraktiken, die sich bei anderen Cyberangriffen als wirksam erwiesen haben, sind:

"Im Jahr 2021 gaben 83 % der Unternehmen an, Phishing-Angriffe erlebt zu haben. Für das Jahr 2022 werden weitere sechs Milliarden Angriffe erwartet." (CyberTalk, 2022)

Validierung und Bereinigung von Eingaben: Suchen Sie nach Escape-Zeichen und anderen Sonderzeichen für die Anwendungssprache und das Betriebssystem, wie z. B. Kommentarzeichen, Zeilenendezeichen und Befehlsbegrenzer. Wenn die Anwendung nur eine begrenzte Anzahl von Werten erwartet, akzeptieren Sie nur diese Werte, z. B. durch Whitelisting oder bedingtes Einschalten.

Vermeiden Sie **anfällige Bewertungskonstrukte**: Wir vermeiden die Verwendung von "eval()" und gleichwertigen Funktionen für rohe Benutzereingaben. CARSA verwendet spezielle sprachspezifische Funktionen, um vom Benutzer gelieferte Argumente sicher zu verarbeiten.

Sperren Sie den Interpreter: Wenn Sie die Kontrolle über die Serverkonfiguration haben, ist es besser, die Interpreterfunktionalität auf das für die Anwendung erforderliche Minimum zu beschränken, um eine Eskalation bis hin zur Injektion von Systembefehlen zu verhindern. Wenn Ihre PHP-Anwendung zum Beispiel die Funktion system() nicht verwendet, können Sie diese Funktion in Ihrer php.ini-Datei deaktivieren, indem Sie sie in der Direktive disable_functions angeben. Üblicherweise deaktivierte Funktionen für PHP sind: exec(), passthru(), shell_exec(), system(), proc_open(), popen(), curl_exec(), curl_multi_exec(), parse_ini_file() und show_source().

Prüfen Sie unseren Code: CARSA nutzte Werkzeuge zur statischen Codeprüfung, um nach Schwachstellen im Zusammenhang mit der Eingabevalidierung und unsicheren Bewertung zu suchen.

Scannen der Anwendungen: Die Organisation verwendet einen Scanner, um sicherzustellen, dass die Anwendungen vor verschiedenen Arten von Angriffen sicher sind. CARSA verfügt zum Beispiel über ein Intrusion Detection System.

ERKENNEN

Der Cyberangriff fand innerhalb von CARSA statt, und die Art des Cyberangriffs war ein **"Phishing-Angriff"**. Der Phishing-Angriff ist eine Art von Social-Engineering-Angriff, der häufig zum Diebstahl von Benutzerdaten, einschließlich der Anmeldedaten, verwendet wird.

Nach dem STRIDE-Modell hat diese Art von Angriff als "Bedrohung" die Erhöhung der Berechtigung, da die verletzte Eigenschaft die "Autorisierung" ist. Bei dieser Art von Cyberangriff erlaubt der Benutzer jemandem, etwas zu tun, wozu er nicht berechtigt ist.

Nach dem MITRE ATT&CK Rahmenwerk ist dieser Angriff:

☑ Aufklären: Phishing für Informationen: Spearphishing-Dienst, Spearphishing-Anhang und Spearphishing-Link.

☑ Erster Zugang: Phishing: Spearphishing Anhänge, Link oder über Service.

☑ Ausführung: Angreifer können Phishing-Nachrichten versenden, um Zugang zu den Systemen der Opfer zu erhalten. Alle Formen des Phishings sind elektronisch übermittelte Social Engineering-Methoden. Phishing kann gezielt erfolgen, was als Spearphishing bezeichnet wird. Beim Spearphishing wird eine bestimmte Person, ein bestimmtes Unternehmen oder eine bestimmte Branche ins Visier des Angreifers genommen. Ganz allgemein können Angreifer auch nicht zielgerichtetes Phishing betreiben, z. B. in Massen-Malware-Spam-Kampagnen.

☑ Entdeckung: Die Entdeckung kann durch folgende Faktoren erfolgen: Anwendungsprotokoll (Inhalt), Datei (Dateierstellung) oder Netzwerkverkehr (Inhalt oder Fluss)

☑ Seitliche Bewegung: Internes Spearphishing

☑ Exfiltration: Social Engineering und Phishing-Angriffe; ausgehende Post, Downloads auf unsichere Geräte, Uploads auf externe Dienste und unsicheres Cloud-Verhalten

☑ Auswirkungen: Verlust sensibler Daten, Rufschädigung, Abwanderung von Klienten oder Kunden, Kosten für Ausfallzeiten usw.

REAGIEREN

WO: Der Angreifer war eine unbekannte externe Person/Organisation über einen CARSA-Mitarbeiter.
WEM: Die Zugangsdaten für eine kostenpflichtige (keine öffentliche oder Open-Source-) Software.
WARUM: Diebstahl von Anmeldedaten und sensiblen Unternehmensdaten.
WAS: Daten und Passwörter
WIE: Ein Mitarbeiter hat Software installiert, die gemäß den Unternehmensrichtlinien nicht erlaubt war. Dieser Typ der Software war unerlaubt wegen zweifelhafte Zuverlässigkeit und Sicherheit. (Allgemein,

alle software die auf den Computern der Mitarbeiter installiert wird, muss vom technischen Personal des Unternehmens beaufsichtigt werden). Diese Software enthielt einen Netz-"Trojaner". Es gibt verschiedene Arten, wie ein Trojaner ein System angreift, in diesem speziellen Fall war es ein "Infostealer-Trojaner", der es, wie es klingt, auf die Daten auf dem infizierten Computer abgesehen hat.

STRATEGIE: Die verfolgte Strategie bestand darin, die Mac-Adresse zurückzuverfolgen, um den infizierten Computer und den verantwortlichen Mitarbeiter zu identifizieren. Später wurden sowohl die Software als auch der Virus entfernt.

WIEDERHERSTELLEN

AUSWIRKUNG: Diebstahl von Benutzerinformationen

WIEDERHERSTELLUNGSSTRATEGIE:

- ☑ Anhand der MAC-Adresse wussten wir, welcher Mitarbeiter angegriffen wurde, ohne dass er es überhaupt bemerkte.
- ☑ Software wurde deinstalliert, die nicht hätte installiert werden dürfen
- ☑ ein Antiviren- und Antimalware-Programm auf dem betreffenden Computer ausgeführt wurde.

Geänderte kompromittierte Benutzeranmeldedaten

BESTE STRATEGIE: der gesamte Computer könnte formatiert worden sein, da man nie sicher sein kann, dass er vollständig entfernt wurde.

LESSONS LEARNT

Stärkung der Verantwortlichkeit der Mitarbeiter durch:

- ☑ Schulung mit Kurzvorträgen über die Wichtigkeit, keine unangekündigte Software zu installieren, und Sicherheitsbestätigung durch das technische Supportteam und,
- ☑ Erinnern Sie sich an die Sicherheitsrichtlinien und Sicherheitsvorschriften im Bereich der Cybersicherheit.
- ☑ Aktualisierung der Software auf den Rechnern des Unternehmens (Software: Windows und Antivirenprogramme). Die Mitarbeiter daran zu erinnern, den Antiviren-Scan mehrmals durchzuführen.

FALLSTUDIE 3: DIE KREDITKARTE IN EINEM KMU ÜBER WIFI NETZWERK

DIE BETROFFENE ORGANISATION

Bodegas Monje befindet sich in einer außergewöhnlichen Enklave der Insel Teneriffa, in dem als "La Hollera" bekannten Ort in der Gemeinde El Sauzal mit Blick auf den Teide. Die Familie Monje kann auf eine lange Weinbautradition seit 1750 zurückblicken. Das Nebeneinander von Eichenfässern und modernen Mazerationsanlagen verleiht den Rot-, Weiß- und Roséweinen einen besonderen Charakter und Geschmack, der perfekt auf die beste Gastronomie der Kanarischen Inseln abgestimmt ist. Diese Weinkellerei bietet auch kulturelle, gastronomische und Freizeitinitiativen an, die die Grenzen des Weins erweitern und ihn in das soziale Umfeld zurückbringen, aus dem er historisch stammt - ein echtes Engagement für den Weintourismus: Wine&Tours**.**

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Methode, mit der die Informationen für diese Fallstudie gesammelt wurden, war ein ausführliches Interview.

VORBEUGEN

Die Organisation wendete vor diesem Ereignis keine Cybersicherheitspraktiken an. Sie verfügen lediglich über eine Firewall beim Internet Service Provider (Router Movistar).

Die spezifischen Sicherheitspraktiken, die in Bodegas Monje eingeführt wurden und die nachweislich zur Verhinderung dieser Art von Vorfällen beigetragen haben, wurden nach dem Vorfall geplant. Die ergriffenen Maßnahmen haben insbesondere dazu beigetragen, weitere Angriffe ähnlicher Art zu verhindern.

IDENTIFIZIEREN

Ein Kunde des Unternehmens griff auf das Unternehmen zu, um die hergestellten Produkte zu konsumieren, und verband sich über das WIFI-Netz mit dem Internet. Der Cyberangriff wurde von dem betroffenen Kunden selbst erkannt. Er entdeckte Bewegungen auf seinen Bankkonten mit Online-Zahlungen, die mit seiner Kreditkarte, aber nicht von ihm selbst getätigt wurden. Alle diese Bewegungen erfolgten kurz nach seinem Besuch bei der Firma "Bodegas Monje".

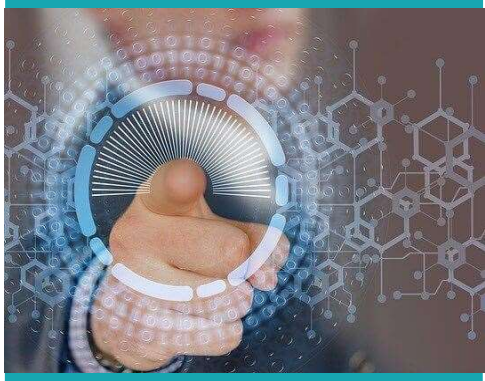
ANTWORTEN

WHO: der eigene Kunde des Unternehmens.
WEM: an einen anderen Kunden über das Unternehmen.
WARUM: um Geld zu stehlen
WAS: sich Bankdaten anzueignen und Abbuchungen vorzunehmen, um von dem Geld anderer zu profitieren
WIE: Infiltration über das Wifi-Netzwerk des Kunden
STRATEGIE: Umgestaltung des Netzes, um die Verbindung der Kunden, die das Geschäft besuchen, vom Zahlungssystem und dem internen Netz des Unternehmens zu trennen.

WIEDERHERSTELLEN

AUSWIRKUNG:

- ☑ Die Kreditkarte eines Kunden der Einrichtung kompromittiert
- ☑ Das Vertrauen der Kunden in die Sicherheit des Unternehmens könnte beeinträchtigt werden, und sie würden sich nicht mehr so leicht auf diese Zahlungsmethode verlassen können.
- ☑ Wenn mehr Kunden von diesem Cyberangriff betroffen wären, würde sich dies direkt auf den Ruf des Unternehmens auswirken.



WIEDERHERSTELLUNGSSTRATEGIE:

Die Strategie des Firmeninhabers bestand ab dem Zeitpunkt, an dem er von dem Vorfall erfuhr, darin, das WLAN abzuschalten und/oder das Gastnetzwerk zu trennen. Dann wandte er sich an ein Cybersicherheitsunternehmen, um das Problem zu lösen.
Die neue Wiederherstellungsstrategie des Cybersecurity-Teams bestand darin, das Netzwerk so umzugestalten, dass das Kundennetzwerk vom internen Netzwerk des Unternehmens getrennt wurde, in dem die sensibelsten Daten (Daten der Mitarbeiter und der Kunden, z. B. Zahlungssystemdaten) gespeichert sind.

Nach der Neugestaltung des Netzes konnte kein gestohlenes Geld wiederbeschafft werden. Der Kunde musste die alte, "gestohlene" Kreditkarte gegen eine neue austauschen. Die Person, die den Cyberangriff durchgeführt hat, konnte nicht identifiziert werden. Es konnten keine rechtlichen Schritte eingeleitet werden.
In dieser Situation gibt es eine bessere Strategie. Anstatt das WLAN-Netz des Unternehmens abzuschalten, hätte man dies auch zusätzlich tun können

- ☑ Erstellung einer Liste aller kompromittierten Informationen, mit allen Kontaktdaten der möglichen Kunden, die betroffen sein könnten (nach Zeitplan - wer war zur gleichen Zeit im Unternehmen wie der betroffene Kunde).

- ☑ Andere Kunden darüber zu informieren, dass sie auf seltsame Bewegungen auf ihren Bankkonten achten sollen, die durch Online-Zahlungen mit ihrer Kreditkarte ausgelöst wurden.
- ☑ Es sollen so viele Informationen wie möglich gesammelt werden, um nicht nur den Verursacher des Cyberangriffs zu ermitteln, sondern auch um Kunden, die ebenfalls betroffen sein könnten, besser warnen zu können.
- ☑ Die Passwörter sofort zu ändern, um eine plötzliche Abschaltung des Unternehmens zu vermeiden, denn zu diesem Zeitpunkt war das Netzwerk nicht geteilt, es funktionierte für Kunden und Mitarbeiter gleichzeitig.

LESSONS LEARNT

Unter den gewonnenen Erkenntnissen sind die folgenden hervorzuheben:

- ☑ dass es besser ist, das Netz zu segmentieren
- ☑ dass eine Null-Vertrauens-Politik umgesetzt werden muss
- ☑ dass man nicht unbedingt ein großes Unternehmen sein muss, um Opfer eines Cyberangriffs zu werden
- ☑ über aktuelle Geräte und aktive Cybersicherheitssysteme (mit professioneller Firewall, IPS, Antivirus usw.) zu verfügen.

FALLSTUDIE 4: INFORMATIONSWEITERGABE HANESBRANDS INC.

BETROFFENE ORGANISATION

Hanesbrands Inc. (HBI) ist ein 1901 gegründetes, multinationales Bekleidungsunternehmen mit Sitz in Winston-Salem, USA. Das Unternehmen hat über 250 Filialen in 47 Ländern. Zu den bekanntesten Marken des Unternehmens gehören Hanes, Champion, Playtex, Bali, L'eggs, Just My Size, Barely There, Wonderbra, Duofold, Celebrity, Maidenform, Zorba, usw. Einer der Wettbewerbsvorteile von Hanesbrands besteht darin, dass 70 % der verkauften Kleidungsstücke sowohl in den eigenen Räumlichkeiten als auch in denen von Partnerunternehmen hergestellt werden. Auf diese Weise gelingt es dem Unternehmen, den größten Teil der Lieferkette zu kontrollieren, was auch die Einführung strenger Nachhaltigkeitspraktiken ermöglicht und zu seinem weltweiten Erfolg beiträgt. Im Jahr 2021 wurde HBI von Ethisphere zu einem der World's Most Ethical Companies ernannt und wurde drei Jahre in Folge in die Barron's 100 Most Sustainable Companies aufgenommen. Um sicherzustellen, dass das Unternehmen eine langfristige Politik der Nachhaltigkeit verfolgt, hat es sich 2030 globale Nachhaltigkeitsziele gesetzt (in Übereinstimmung mit den Zielen für nachhaltige Entwicklung der Vereinten Nationen unter drei Säulen: People, Planet und Product) und eine Nachhaltigkeits-Website eingerichtet.

Im Jahr 2019 erzielte das Unternehmen einen Umsatz von 7,0 Mrd. USD und beschäftigte rund 61 000 Mitarbeiter. Berichten zufolge gibt HBI mehr als 100 000 USD für Cybersicherheit aus und nutzt dabei hauptsächlich Produkte von Akamai, z. B. Cloud-Dienste.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Methode, die zur Sammlung der Informationen für diese Fallstudie angewandt wurde, war Desk Research; die spezifischen Informationsquellen sind im Abschnitt Referenzen dieses Dokuments zu finden.

"Einem neuen Bericht von Blumira und IBM zufolge dauert der durchschnittliche Lebenszyklus von Sicherheitsverletzungen 287 Tage, wobei Unternehmen 212 Tage benötigen, um eine Sicherheitsverletzung zu entdecken und 75 Tage, um sie einzudämmen." (VentureBeat, 2022)

VORBEUGEN

☑ **Praktiken, die keinerlei Auswirkungen hatten:** Authentifizierung auf der Website - Um seine/ihre Bekleidungsbestellung verfolgen zu können, erhielt der Nutzer einen Link, um sich als Gast auf der Website anzumelden. Der Gastnutzer hatte weitreichende Rechte, um Informationen über die Bestellungen aller anderen Nutzer zu erhalten, indem er einfach die Gast-URL änderte. Daher wurde die Datenbank über die Website kompromittiert, da sie keine Authentifizierung verlangte und den Gastbenutzer als gültigen Benutzer betrachtete. Die für andere Kunden sichtbaren Daten bestanden aus Namen, letzten Ziffern ihrer Kreditkarten, Adresse, Telefonnummer usw.

☑ **Praktiken, die sich bei echten Cyberangriffen dieser Art bewährt haben:**

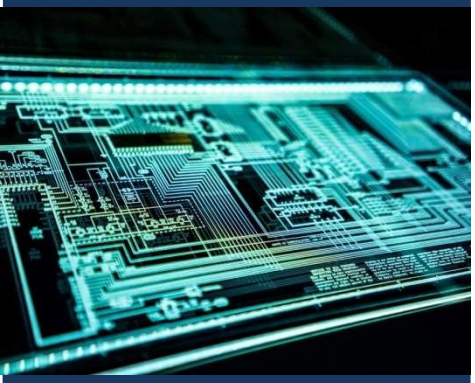
1. Entdeckung der Datenexposition (mit externen Scansystemen).
2. Starke Authentifizierung (Einzelanmeldung, die es einem Benutzer ermöglicht, sich in mehreren verschiedenen Systemen anzumelden, oder unterschiedliche Benutzernamen/Kennwörter für jedes System).
3. Priorisierung des Datenzugriffs (z.B. benötigt die Personalabteilung nur Zugriff auf Mitarbeiterinformationen und die Buchhaltungsabteilung nur Zugriff auf Budget- und Steuerdaten. Gastnutzer sollten prinzipiell nur minimalen Datenzugang haben).
4. Einsatz von Überwachungsinfrastrukturen und automatisierten Lösungen, mit denen potenzielle Probleme schnell erkannt werden können, bevor sie sich zu Notfällen entwickeln, infizierte Datenbanken isoliert werden können und die Support- und IT-Teams für die nächsten Schritte informiert werden können.

IDENTIFIZIEREN

Bei dem Angriff auf Hanesbrands Inc. handelte es sich um eine **Offenlegung von Informationen.**

In der letzten Juniwoche und am ersten Juli 2015 wurde Hanesbrands Inc. Opfer eines Cyberangriffs. Nachdem die Daten gestohlen worden waren, wurde das Unternehmen von den Angreifern über die Sicherheitsverletzung informiert, ohne dass sie ein Motiv für ihr Vorgehen nannten. Es ist sehr wahrscheinlich, dass die Schwachstelle des Unternehmens durch Scannen entdeckt wurde[1]. Die Hacker erstellten auf der Website von

Hanesbrands[2] eine "Gast"-Bestellung (ohne sich auf der Website zu registrieren). Mit dem erhaltenen Bestell-Link gelang es den Hackern, die Datenbank des Unternehmens zu entleeren, in der die Daten aller Kundenbestellungen gespeichert waren (Bestellungen, die auf der Website oder per Telefon aufgegeben wurden) - wie sich herausstellte, konnte der "Gast"-Kassen-Link ohne Authentifizierung auf jede andere Bestellung zugreifen. Innerhalb einer Woche gelang es den Angreifern, an die Daten von über 900 000 Kunden zu gelangen. Um nicht entdeckt zu werden, nutzten die Hacker höchstwahrscheinlich Port Knocking[3], um ihre Aktivitäten zu verschleiern. Laut Hanesbrands haben die Angreifer Screenshots[4] verwendet, um die Daten zu extrahieren. Es ist jedoch sehr wahrscheinlich, dass sie einen automatisierten Weg gewählt haben - beispielsweise ein Skript, das die Daten direkt analysiert[5].



Der Angriff wird im MITRE ATT&CK Framework beschrieben:
[1] Aktives Scannen: Scannen auf Schwachstellen (T1592.002).
[2] Erster Zugriff: Ausnutzen der öffentlich zugänglichen Anwendung (T1190).
[3] Persistenz: Verkehrssignalisierung: Port-Knocking (T1205.001).
[4] Bildschirmaufzeichnung (T1113).
[5] Automatisierte Erfassung (T1119).
Der Angriff wurde von dem Unternehmen erkannt, nachdem es von den Angreifern benachrichtigt wurde. Hanesbrands wusste nicht, dass dies geschah, bis die Hacker es ihnen mitteilten.

REAGIEREN

Im Juni 2015 wurde Hanesbrands Inc. von den Angreifern über den Einbruch informiert. Den Angreifern war es gelungen, über ein Gastkonto auf der Website des Unternehmens die allgemeinen Benutzerdaten von 900 000 Kunden zu erlangen. Nachdem Hanesbrands über das Leck informiert wurde, fügte das Unternehmen eine Authentifizierung zu seiner Datenbank "Kundenbestellungen" hinzu und entfernte die Option "Gast-Check-out" (obwohl sie diese behoben hat).

WER: Unbekannt

WEM: Hanesbrands Inc.

WARUM: Es handelte sich um einen gezielten Angriff, um an Informationen über Kundendatenbanken und Kundenlisten zu gelangen, aber die Angreifer haben kein Lösegeld gefordert. Sie haben Hanesbrands lediglich darüber informiert, dass sie die Daten erhalten haben.

WAS: Allgemeine Kundendaten von 900.000 Kunden - Namen, Adressen, Informationen über den Bestellstatus, Telefonnummern und die letzten vier Ziffern der Kreditkarte des Kunden. Die Benutzernamen oder

Passwörter der Kunden wurden jedoch nicht offengelegt. Die Hacker sind nicht in die Unternehmenssysteme von Hanesbrands eingedrungen.

WIE: Die Angreifer erstellten eine Bestellung über ein Gastkonto auf der Website von Hanesbrands. Indem sie sich als "Gast" ausgaben, der eine Bestellung überprüft (die Angreifer waren nicht auf der Website registriert), gelang es ihnen, eine Lücke in der Datenbank von Hanesbrands zu finden, indem sie den Link der Bestellung ausnutzten. Die Hacker konnten auf die Bestelldaten und den Bestellstatus der Kunden zugreifen und die Daten extrahieren.

STRATEGIE: Nachdem Hanesbrands von den Angreifern über die Sicherheitslücke informiert wurde, fügten sie ihrer Datenbank eine Authentifizierung hinzu, um das Informationsleck zu schließen. Darüber hinaus wurde die "Gastbenutzer"-Kasse repariert, über die das Leck verwaltet wurde. Hanesbrands informierte seine Kunden per E-Mail und Post über die Sicherheitsverletzung. Seit diesem Vorfall investiert Hanesbrands jedes Jahr mehr und mehr in die Cybersicherheit.

WIEDERHERSTELLEN

☑ **AUSWIRKUNG:** Die Folgen waren das Durchsickern von allgemeinen Kundeninformationen. Es ist nicht bekannt, ob es zu Klagen oder anderen direkten Schäden gekommen ist.

☑ **WIEDERHERSTELLUNGSSTRATEGIE:** Hanesbrands hat seine Kunden über die Sicherheitsverletzung informiert. Sie reparierten den "Gastbenutzer"-Link[1], um keinen direkten Zugriff auf die Datenbank zu haben, und deaktivierten ihn insgesamt als Option[2]. Bietet einen Kundendienst an, der bei Bedenken der Nutzer antwortet. Darüber hinaus führte das Unternehmen ein Sicherheitsaudit[3] und eine Schwachstellenprüfung[4] seiner bestehenden Systeme durch und investierte in Cybersicherheitsschulungen[5].

Die im MITRE ATT&CK-Rahmen beschriebenen Abhilfemaßnahmen:
[1] Software-Konfiguration (M1054).
[2] Deaktivieren oder Entfernen einer Funktion oder eines Programms (M1042).
[3] Überprüfung (M1047).
[4] Scannen auf Schwachstellen (M1016).
[5] Anleitung für Anwendungsentwickler (M1013).

BESSERE STRATEGIE: Nach der Reparatur des "Gastbenutzer"-Links, über den ein Kunde seinen Einkauf überprüfen konnte, hat Hanesbrands diese Option deaktiviert. Stattdessen hätten sie eine Überwachung auf verdächtige Aktivitäten und/oder Richtlinien für die Überprüfung nur einer bestimmten Menge von Einkäufen hinzufügen können.

LESSONS LEARNT

Angriffe auf die Offenlegung von Informationen sind sehr selten geworden, da viele moderne Tools automatische Cybersicherheit bieten und Unternehmen darauf hinweisen, was ein potenzielles Leck sein könnte. Der Angriff auf Hanesbrands zeigt, dass schwache Datenbankprüfpfade und mangelndes Sicherheitswissen relativ leicht ausgenutzt werden können. In vielen Fällen wird in Datenbanken eingebrochen, weil das Fachwissen im Bereich der Cybersicherheit unzureichend ist und nicht-

technische Mitarbeiter nicht entsprechend geschult werden, so dass sie grundlegende Sicherheitsregeln für Datenbanken verletzen können. Dem IT-Personal könnte auch das nötige Fachwissen fehlen, um Sicherheitsrichtlinien durchzusetzen und angemessene Verfahren und Maßnahmen zur Meldung von Vorfällen durchzuführen.

Ein weiterer Punkt ist, dass die Datenbank in Hanesbrand aufgrund einer Fehlkonfiguration verwundbar war - Datenbanken werden dadurch normalerweise völlig ungeschützt. Es wird oft vergessen, dass es sich bei den Angreifern in der Regel um hochprofessionelle IT-Spezialisten handelt, die sicherlich wissen, wie man solche Schwachstellen ausnutzt. Dem kann durch die Deaktivierung der Standard-Datenbankkonten in Kombination mit geschultem und erfahrenem IT-Personal entgegengewirkt werden.

Hanesbrands hatte Glück, dass nur allgemeine Informationen durchgesickert sind und dass die Angreifer das Unternehmen informiert haben, nachdem sie alle Daten extrahiert hatten, die sie finden konnten. Darüber hinaus hat Hanesbrands seine Kunden sofort über die Sicherheitsverletzung informiert, was zeigt, dass das Unternehmen seinen Kunden gegenüber aufgeschlossen ist und das Problem ernst nimmt.

FALLSTUDIE 5: SPOOFING HUMANA

BETROFFENE ORGANISATION

Humana ist ein Krankenversicherungsunternehmen mit Hauptsitz in Louisville, Kentucky. Ursprünglich wurde das Unternehmen 1961 als Betreiber von Pflegeheimen gegründet. In den 1980er Jahren ging das Unternehmen dazu über, Krankenhäuser zu besitzen und zu verwalten, um dann Krankenversicherungspläne anzubieten. Im Mai 2015 schätzte Forbes den Wert des Unternehmens auf 26,7 Milliarden Dollar. Im Jahr 2020 hatte Humana einen Umsatz von 77,155 Milliarden Dollar und beschäftigte rund 48 000 Mitarbeiter. Monatlich gibt Humana mehr als 100 000 Dollar für Cybersicherheit aus. Humana nutzt Cybersicherheitsprodukte wie "Akamai" (Cloud-Delivery-Plattform) und "Prolexic" (Sicherheitslösungen zum Schutz von Websites, Rechenzentren und IP-Unternehmensanwendungen vor DDoS-Angriffen (Distributed Denial of Service)), "Proofpoint" (Lösung zum Schutz Ihrer Mitarbeiter und kritischen Daten vor fortgeschrittenen E-Mail-Bedrohungen), "Alert Logic" (White-Glove-Managed-Detection-and-Response-Programme) und andere.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Methode, mit der die Informationen für diese Fallstudie gesammelt wurden, war die Sekundärforschung; die spezifischen Informationsquellen sind im Abschnitt Referenzen dieses Dokuments zu finden.

VORBEUGEN

☑ Praktiken, die keinerlei Auswirkungen hatten: Warnungen bei fehlgeschlagenen Anmeldeversuchen - Humana wandte diese Praxis vor dem Vorfall an. Sie war nicht wirksam, da das Unternehmen etwa einen Tag brauchte, um Maßnahmen als Reaktion auf die zahlreichen fehlgeschlagenen Anmeldeversuche zu ergreifen

☑ **Praktiken, die sich bei echten Cyberangriffen bewährt haben:**

1. Kontosperrung nach fehlgeschlagenem Anmeldeversuch.
2. Blockierung des Internetverkehrs aus Ländern, mit denen die Organisation keine Geschäfte tätigt.
3. Erzwingen eines Passwort-Resets.

IDENTIFIZIEREN

Der Angriff auf Humana war vom **Typ Spoofing.**

Am 3. Juni 2018 war Humana Ziel eines ausgeklügelten Cyber-Spoofing-Angriffs, der auf Humana.com stattfand. Am selben Tag wurde Humana auf einen signifikanten Anstieg der Login-Fehlversuche von IP-Adressen aus dem Ausland aufmerksam[1]. Um ihren tatsächlichen Standort nicht preiszugeben, verwendeten die Angreifer Multi-Hop-Proxies[2]. Das Volumen der Anmeldeversuche bei Humana.com deutet darauf hin, dass ein großer und breit angelegter Angriff gestartet wurde. Die Art des Angriffs und die beobachteten Verhaltensweisen deuteten darauf hin, dass der Angreifer über eine große Datenbank mit Benutzeridentitäten und entsprechenden Passwörtern verfügte, die mit der Absicht eingegeben wurden, durch "Brute-Force"[3] herauszufinden, welche davon auf Humana.com gültig sein könnten. Die übermäßige Anzahl von Anmeldefehlern deutet darauf hin, dass die Anmeldeinformationen nicht von Humana[4] stammen (und höchstwahrscheinlich aus dem "dunklen" Web gekauft wurden). Am 4. Juni blockierte Humana die IPs. Auf der Grundlage dieser Fakten kann dies als Identitätsspoofing-Angriff bezeichnet werden. Die Angreifer sammelten Daten[5] von etwa 65 000 Nutzern, darunter:

☑ Medizinische, zahnmedizinische und visuelle Ansprüche einschließlich der erbrachten Leistungen, Name des Anbieters, Daten der Leistung, Kosten und bezahlte Beträge usw.

☑ Informationen zu Ausgabenkonten, wie z. B. Informationen zu Ausgaben und Guthaben auf Gesundheitskonten.

☑ Humana hatte nach dem Vorfall zusätzliche Maßnahmen ergriffen, wie die Sperrung des Kontos nach einem fehlgeschlagenen Anmeldeversuch, die Sperrung des Internetverkehrs aus Ländern, mit denen das Unternehmen keine Geschäfte macht, und die erzwungene Zurücksetzung des Passworts.

Der Angriff wird vom MITRE ATT&CK Framework beschrieben:

[1] Befehls- und Scripting-Interpreter: Netzwerkgeräte-CLI (T1059.008).
[2] Proxy: Multi-hop Proxy (T1090.003).
[3] Brute Force: Ausfüllen von Zugangsdaten (T1110.004).
[4] Sammeln von Informationen über die Identität des Opfers: Berechtigungsnachweise (T1589.001).
[5] Automatisierte Erfassung (T1119).
Der Angriff wurde durch Warnungen für Fehler bei mehreren Anmeldeversuchen erkannt.

RESPOND

☑ **WER:** Unbekann
☑ **WEM:** Humana
☑ **WARUM:** Identitätsdiebstahl (der wahrscheinlich an Dritte verkauft wird)
☑ **WAS:** Sensible Nutzerdaten (medizinische, zahnmedizinische und visuelle Ansprüche, einschließlich der erbrachten Leistungen, Name des Anbieters, Daten der Leistungen, Kosten und bezahlte Beträge usw.; Informationen zu den Kostenkonten, wie z. B. Informationen zu den Ausgaben und dem Saldo von Gesundheitskonten)
☑ **WIE:** Die Angreifer sammelten große Mengen von Konten und Anmeldedaten. Mit Hilfe von Multi-Hop-Proxys erzwangen sie dann die Anmeldung mit den Konten, die sie hatten. Nach erfolgreicher Anmeldung sammelten die Angreifer Benutzerdaten durch kleine Datenübertragungen.
☑ **STRATEGIE:** Als Humana den erheblichen Anstieg der Fehler bei den Anmeldeversuchen bemerkte, sperrten seine Cybersicherheitsbeauftragten die ausländischen IP-Adressen, von denen aus die mehrfachen Anmeldeversuche unternommen wurden. Danach erzwang Humana die Rücksetzung der Passwörter für alle Konten, bei denen die Sicherheitslücke bekannt war, und brachte sogar ein Produkt heraus, das den Mitgliedern ein Jahr lang Schutz vor Identitätsdiebstahl bot.

WIEDERHERSTELLEN

☑ **AUSWIRKUNG:** Die Folge war das Durchsickern vertraulicher Informationen von Nutzern (medizinische, zahnmedizinische und visuelle Ansprüche, einschließlich erbrachter Leistungen, Name des Anbieters, Leistungsdaten, Gebühren und gezahlte Beträge usw.; Informationen über Ausgabenkonten, wie z. B. Informationen über Ausgaben und Guthaben von Gesundheitskonten). Daraufhin wurden zahlreiche Klagen wegen Fahrlässigkeit gegen Humana eingereicht. Es gibt keine Informationen darüber, ob das Unternehmen die Klagen gewonnen hat, was darauf schließen lässt, dass die Ergebnisse wahrscheinlich negativ waren.

☑ **WIEDERHERSTELLUNGSSTRATEGIE:** Humana benachrichtigte eine Reihe von Mitgliedern, um sie über die Datenverletzung zu informieren, nachdem ein Monat vergangen war. Das Unternehmen hat außerdem eine Reihe von Maßnahmen zur Verbesserung der Cybersicherheit ergriffen, darunter: 1) Erzwingen eines Passwort-Resets[1]; 2) Einführung neuer Warnmeldungen für erfolgreiche und fehlgeschlagene Anmeldungen[2] und 3) Sperren von Konten, die mit verdächtigen Aktivitäten in Verbindung gebracht wurden[3]. Darüber hinaus wurde eine Reihe von technischen Maßnahmen zur Verbesserung der Sicherheit des Webportals ergriffen (Blockierung von Brute-Force-Angriffen, Schutz vor SQL-Injektionen[4], Installation eines SSL-Sicherheitszertifikats[5] usw.). Das Unternehmen sperrte auch alle ausländischen IP-Adressen, die für seine Tätigkeit nicht relevant waren[6].

☑

Die von Humana getroffenen Abhilfemaßnahmen sind im **MITRE ATT&CK-Framework** beschrieben:
[1] Passwort-Richtlinien (M1027).
[2] Schutz vor Eindringlingen in das Netzwerk (M1031).
[3] Richtlinien für die Kontonutzung (M1036).
[4] Software-Konfiguration (M1054).
[5] SSL/TLS-Prüfung (M1020).
[6] Netzwerkverkehr filtern (M1037).

BESSERE STRATEGIE:

Humana hätte die Benutzer früher benachrichtigen können. Sie hätten auch zusätzliche Sicherheitsmaßnahmen ergreifen können, wie zum Beispiel:

- Verwendung einer Authentifizierung auf der Grundlage eines Schlüsselaustauschs zwischen den Rechnern im Netzwerk einer Organisation oder einer Multi-Faktor-Authentifizierung für den Fernzugriff;
- Verwendung einer Zugriffskontrollliste, um private IP-Adressen auf nachgelagerten Schnittstellen zu sperren;
- Implementierung der Filterung von ein- und ausgehendem Datenverkehr;
- Konfiguration von Routern und Switches - wenn möglich - zur Zurückweisung von Paketen, die von außerhalb des lokalen Netzwerks einer Organisation stammen und vorgeben, von innerhalb zu stammen;
- Aktivierung von Verschlüsselungssitzungen auf dem Router einer Organisation, so dass vertrauenswürdige Hosts außerhalb ihres Netzes sicher mit ihren lokalen Hosts kommunizieren können.

LESSONS LEARNT

Die Lehren, die daraus gezogen wurden, sind die Notwendigkeit, sich stärker auf die Sicherung der persönlichen Daten der Nutzer zu konzentrieren, Schulungen für die Mitarbeiter zu organisieren, um das Bewusstsein für Cyber-Bedrohungen zu schärfen, und die Nutzer über Datenlecks zu informieren, da es nach dem Vorfall zahlreiche Klagen wegen Fahrlässigkeit gegen Humana gab (Humana gab erst einen Monat später bekannt, dass ein solcher Angriff stattgefunden hatte).

Die Auswirkungen des Angriffs waren nicht nur mit den Kosten für die Bewältigung des Angriffs und der Klagen verbunden, sondern auch mit dem großen Schaden für den Ruf von Humana und seine Zuverlässigkeit. Da das Unternehmen im Bereich der Krankenversicherung tätig ist, ist es von entscheidender Bedeutung, dass es über die höchsten Sicherheitsmaßnahmen verfügt und das Vertrauen seiner Kunden genießt, da die in seinen Systemen gespeicherten Daten sehr sensibel und vertraulich sind. Aus diesem Grund war und ist Humana schon lange vor dem in diesem Fall beschriebenen Angriff und auch danach ein beliebtes Ziel von Cyberangriffen. In Anbetracht dessen könnte die Fehleinschätzung der Schwere dieses Angriffs als überraschend angesehen werden.

FALLSTUDIE 6: DENIAL OF SERVICE WILLIAM HILL

BETROFFENE ORGANISATION

William Hill ist ein Online-Glücksspielunternehmen mit Sitz in London, England - ursprünglich 1934 von William Hill gegründet. Das Unternehmen wechselte viele Male den Besitzer - 1971 wurde es zum ersten Mal von Sears Holdings gekauft. Nach zahlreichen Verkäufen wurde es im April 2021 von Ceasars Entertainment übernommen. Im Jahr 2020 erzielte das Unternehmen einen Umsatz von 1.324,3 Millionen Pfund und beschäftigte 12.000 Mitarbeiter (8.000 im Vereinigten Königreich). 2019 begann das Unternehmen mit der Schließung von mehr als 800 Wettbüros aufgrund geringer Gewinne, behauptete aber, das Personal zu behalten.

Monatlich gibt William Hill über 100.000 Dollar für Cybersicherheit aus. Das Unternehmen nutzt Cybersicherheitsprodukte wie "Prolexic" (Sicherheitslösungen zum Schutz von Websites, Rechenzentren und IP-Anwendungen von Unternehmen vor DDoS-Angriffen (Distributed Denial of Service))", "Proofpoint" (Lösung zum Schutz von Mitarbeitern und kritischen Daten vor fortschrittlichen E-Mail-Bedrohungen), "F5 BIG-IP Application Security Manager" (flexible Web Application Firewall, die Webanwendungen in traditionellen, virtuellen und privaten Cloud-Umgebungen schützt) Check Point" (schützt seine Kunden vor Cyberangriffen der 5. Generation mit einer branchenführenden Erkennungsrate von Malware, Ransomware und hochentwickelten gezielten Bedrohungen), usw.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Methode, die zur Sammlung der Informationen für diese Fallstudie angewandt wurde, war Desk Research; die spezifischen Informationsquellen sind im Abschnitt Referenzen dieses Dokuments zu finden.

VORBEUGEN

☑ **Praktiken, die keine Auswirkungen hatten:**

1. Anycast-Netzwerkdiffusion - William Hill verfügt über diese Art der Verteidigung, die nützlich ist, um enorme Mengen an Kunden zu halten, die seine Website besuchen, oder um große Mengen an unerwünschtem Netzwerkverkehr (wie bei DDoS-Angriffen) aufzulösen. Diese Strategie funktioniert in der Regel in den meisten Fällen von DDoS-Angriffen.
2. Die einfache Erhöhung der Bandbreite des Netzes (wie viel Datenverkehr es aufnehmen kann) hat sich bei diesem Angriff nicht als wirksam erwiesen.

☑ **Praktiken, die sich bei echten Cyberangriffen dieser Art bewährt haben:**

1. Implementierung eines DDoS-Schutzes auf Serverebene - zusätzliche Regeln, die helfen, bösartigen Netzwerkverkehr zu identifizieren und zu blockieren.

2. Hinzufügen von Anycast-Netzwerken von Drittanbietern - dies kann Unternehmen dabei helfen, ihre Fähigkeit zur Bewältigung von wesentlich mehr Netzwerkverkehr oder DDoS-Angriffen enorm zu steigern.

"Laut Cloudflare erhielt die Fertigungsindustrie im vierten Quartal 2021 die meisten DDoS-Angriffe auf der Anwendungsebene und verzeichnete einen Anstieg der Anzahl der Angriffe um 641 % im Vergleich zum Vorquartal." (Cook, 2022)

IDENTIFiZIEREN

Die Attacke gegen William Hill war ein **Denial of Service Type.**

Am 1. November 2016 war William Hill das Ziel eines hochleistungsfähigen verteilten Denial-of-Service-Angriffs[1]. Vor dem Angriff sammelten die Angreifer Informationen über die Netzwerkdetails der Website von William Hill[2]. Danach überschwemmten die Angreifer die Website von William Hill mit Datenverkehr, so dass sie nicht mehr richtig funktionieren konnte. Der Angriff verhinderte, dass Kunden Wetten für die Spiele der UEFA Champions League am Dienstagabend platzieren konnten. Der Angriff auf William Hill wurde mit Hilfe einer Malware namens "Mirai"[4] durchgeführt, die ein Netzwerk aus zahlreichen Computersystemen erstellt, das als "Botnet"[3] bezeichnet wird, um den DDoS-Angriff über diese Systeme zu starten.

Der Angriff wird vom MITRE ATT&CK Framework beschrieben:

[1] Network Denial of Service: Direkte Netzwerküberflutung (T1498.001).

[2] Sammeln von Netzwerkinformationen des Opfers: IP-Adressen (T1590.005).

[3] Aneignung der Infrastruktur: Botnetz (T1583.005).

[4] Sich selbst verbreitender Wurm-Virus, der eine Datenbank mit Standard-Anmeldeinformationen verwendet. Mit diesen Anmeldeinformationen werden IoT-Geräte (intelligente Geräte wie Fitness-Tracker, Sprachassistenten, Smarthome-Zubehör usw.) gescannt und infiziert.

Der Angriff wurde erkannt, nachdem die Website von William Hill nicht mehr reagierte und nicht mehr zugänglich war.

ANTWORT

WER: Unbekannt.
WEM: William Hill.
WARUM: Geschäftsfehden - es ist sehr wahrscheinlich, dass Firmenkonkurrenten solche Aktionen durchführen, besonders in Zeiten populärer Sportereignisse wie der UEFA Champions League / Erpressung - wenn William Hill die Situation nicht in den Griff bekommt, ist es wahrscheinlich, dass Lösegeld gefordert wird.

WAS: Die Website von William Hill war 24 Stunden lang nicht erreichbar, was Verluste in Höhe von 4,4 Millionen Pfund verursachte. Es dauerte Tage, bis William Hill seine Website und Systeme vollständig wiederherstellen konnte.

WIE: Auf der Website von William Hill wurde ein hochleistungsfähiger Distributed-Denial-of-Service-Angriff mit einem "Botnet"-Netzwerk durchgeführt (mehrere Computer, die mit einem Malware-Virus infiziert waren und zur Durchführung eines solchen Angriffs ohne ihr Wissen oder ihre Zustimmung verwendet wurden), das von einer Malware namens "Mirai" erstellt wurde.

STRATEGIE: Nachdem die IT-Spezialisten von William Hill festgestellt hatten, dass ihre Website nicht funktioniert, begannen sie, den eingehenden Datenverkehr zu filtern. William Hill nutzte die Anycast-Netzwerkdiffusion, bei der der Netzwerkverkehr über das Netzwerk der Unternehmensserver gestreut wird. Diese Abschwächung verteilt den Netzwerkverkehr bis zu dem Punkt, an dem er vom Unternehmensnetzwerk absorbiert wird. Die Nützlichkeit dieser Strategie hängt davon ab, wie groß das Netzwerk des Unternehmens ist und wie groß der DDoS-Angriff ist. Im Fall von William Hill – selbst eine erstklassigen Infrastruktur und Sicherheit war nicht genug eine solche Attacke abzuwehren.

WIEDERHERSTELLEN

AUSWIRKUNG: Der DDoS-Angriff auf William Hill führte dazu, dass die Website des Unternehmens über 24 Stunden lang nicht erreichbar war und die Kunden nicht auf die Spiele der UEFA Champions League wetten konnten. Dies führte zu Verlusten von über 4,4 Millionen Pfund an einem einzigen Tag. Glücklicherweise wurde nur die Website von William Hill angegriffen, so dass die sensiblen Daten der Nutzer unversehrt blieben (was ein Hinweis darauf ist, dass die Angreifer die Nutzer vom Besuch der Website abhalten wollten, und nicht, um Daten zu stehlen). Die IT-Spezialisten von William Hill arbeiteten mehr als 4 Tage rund um die Uhr, um die Website und die betroffenen Systeme wiederherzustellen.

WIEDERHERSTELLUNGSSTRATEGIE: Um dem Angriff zu begegnen, filterte William Hill den eingehenden Netzwerkverkehr[1]. Filterung des Netzwerkverkehrs - Blockierung des reinen Angriffsverkehrs und Zulassung des legalen Verkehrs. Außerdem begann William Hill mit der Nutzung von Drittanbietern von Anycast-Netzwerkdiensten (Unternehmen, die diese Art von Diensten anbieten, die den DDoS-Angriff auflösen, indem sie den gesamten eingehenden Datenverkehr über ihr Netzwerk streuen).

BESSERE STRATEGIE:

☑ Host-Gesundheitsprüfung, die die IT-Spezialisten des Unternehmens alarmiert, wenn eine abnormale Netzwerknutzung festgestellt wird [2]. Werden diese rechtzeitig erkannt, können

Maßnahmen ergriffen werden, um die Verfügbarkeit der Website zu gewährleisten.

☑ Es kann "Blackhole Routing" verwendet werden. Dabei handelt es sich um eine Technik, bei der sowohl der rechtmäßige als auch der bösartige Datenverkehr auf eine Null-Route geleitet und aus dem Netz entfernt wird. Dies ist keine ideale Lösung, da die Website dadurch unzugänglich wird.

☑ Ratenbegrenzung. Sie begrenzt die Anzahl der Anfragen, die der Server empfangen kann - sie allein kann den DDoS-Angriff nicht stoppen, aber sie ist ein nützliches Instrument in der allgemeinen Verteidigungsstrategie.

Die im MITRE ATT&CK-Rahmen beschriebene Wiederherstellungsstrategie:

a. [1] Filtern des Netzwerkverkehrs (M1037).
b. [2] Sensor Health: Host-Status (DS0013).

LESSONS LEARNT

Der Angriff auf William Hill zeigt uns, dass selbst ein Unternehmen mit hervorragender Cybersicherheit, das auf derartige Angriffe vorbereitet ist, darunter leiden kann. Obwohl die Website des Unternehmens durch den DDoS-Angriff lahmgelegt wurde (normalerweise sind solche Angriffe nur ein Vorwand für den eigentlichen Angriff), war die Sicherheit auf höchster Ebene intakt und funktionierte, so dass die sensiblen Daten der Kunden sicher waren. Das zeigte den Kunden, dass sie sicher sind, und bewahrte die Glaubwürdigkeit des Unternehmens. Die Tatsache, dass die Angreifer nicht weiter versuchten, die Schwachstelle von William Hill auszunutzen, deutet darauf hin, dass der Angriff höchstwahrscheinlich aus geschäftlicher Rivalität (konkurrierende Unternehmen, die den Wettmarkt ausnutzen wollen) oder als Erpressungsversuch erfolgte (das Unternehmen ist auf seine Website angewiesen, und wenn die Angreifer sie lahmlegen, entstehen Verluste).

Mit dem Eintritt in die Ära der intelligenten Geräte (IoT), in der alles aus der Ferne gesteuert werden kann (Smart-Home-Lampen, Staubsauger, Kühlschränke, intelligente Uhren usw.), müssen wir auch über die Sicherheit nachdenken, die angewendet werden muss. Alle diese intelligenten Geräte haben eine IP-Adresse und können über das Netzwerk gehackt werden, um Informationen zu erhalten oder "zombifiziert" zu werden (Ihr Gerät wird ohne Ihr Wissen gesteuert und verhält sich seltsam) und für DDoS-Angriffe zur Überflutung einer Website verwendet werden.

FALLSTUDIE 7: COBALT STRIKE: DER EINSATZ VON RED-TEAMING-TOOLS DURCH CYBERKRIMINELLE

BETROFFENE ORGANISATION

Cobalt Strike ist ein Red-Team-Tool, das im Jahr 2012 entwickelt wurde. Sein Hauptzweck besteht darin, Red Teams beim Testen und Simulieren von Cyberangriffen zu unterstützen. Da das Tool über gute Fähigkeiten verfügt, Sicherheitsgrenzen durch Umgehungen zu umgehen, haben Angreifer einige seiner Versionen gekapert, um es als Übertragungswerkzeug für bösartige Nutzlasten wie Ransomware zu missbrauchen. Diese Fallstudie konzentriert sich nicht auf ein einzelnes Unternehmen, da Cobalt Strike in freier Wildbahn eingesetzt wird, um Massenangriffe auf verschiedene Arten von Organisationen wie Hersteller, Finanzinstitute, Telekommunikationsunternehmen und andere durchzuführen

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Methode, die zur Sammlung der Informationen für diese Fallstudie angewandt wurde, war Desk Research; die spezifischen Informationsquellen sind im Abschnitt Referenzen dieses Dokuments zu finden.

VORBEUGEN

Die Erkennung und Abwehr eines Angriffs, bei dem das Red-Teaming-Tool Cobalt Strike zum Einsatz kommt, umfasst eine Sicherheitskette über die gesamte Infrastruktur. Diese beginnt bereits mit der Schutz- und Überwachungssoftware auf dem Endpunkt-Client und reicht bis zur Netzwerkebene. Darüber hinaus ist eine aktive Bedrohungsanalyse erforderlich, um signaturbasierte Erkennungswerkzeuge auf dem neuesten Stand zu halten.

Dies beinhaltet in der Regel:

- ☑ Endgerätesicherheit (z. B. Antivirus, hostbasierte Überwachung)
- ☑ Netzwerksicherheit (z. B. Firewall, Proxy, Erkennung von Signaturen/Mustern im Datenverkehr)
- ☑ E-Mail-Sicherheit
- ☑ Korrekt konfigurierte Host-/Sicherheitsrichtlinien

IDENTIFIZIEREN

Cobalt Strike ist ein multifunktionales kommerzielles Tool, das verschiedene Angriffstechniken erfüllt. Betrachtet man das Tool

und seine Fähigkeiten, so kann es als Informationsoffenlegung und Erhöhung von Rechten kategorisiert werden. Da es jedoch auch zum Absetzen weiterer bösartiger Nutzdaten verwendet werden kann, insbesondere da Ransomware-Angriffe in Kombination mit Cobalt Strike beobachtet wurden, kann die Liste um Manipulation und Denial of Service erweitert werden.

In Anbetracht aller Funktionen des Tools handelt es sich um ein Fernzugriffstool mit lateralen Bewegungsmöglichkeiten. Dies führt zu einer umfangreichen Liste von Angriffstechniken, die von Cobalt Strike verwendet werden, und daher werden wir hier nur einige davon behandeln.

- ☑ Missbrauch des Elevation Control Mechanism (T1548)
- ☑ Sobald Cobalt Strike auf einem System ausgeführt wurde, ist es in der Lage, verschiedene Techniken auszuführen, um höhere Berechtigungen zu erhalten.
- ☑ BITS-Aufträge (T1197)
- ☑ BITS ist ein Windows-Tool, das von Cobalt Strike zum Herunterladen von Nutzdaten verwendet werden kann.
- ☑ Befehls- und Scripting-Interpreter (T1059)
- ☑ Cobalt Strike kann verschiedene Tools verwenden, um Befehle, Code und Skripte auszuführen. Dazu gehören PowerShell, Windows Command Shell, Visual Basic, Python und JavaScript.
- ☑ Ausnutzung für die Ausweitung von Privilegien (T1068)
- ☑ Um höhere Privilegien zu erlangen, kann Cobalt Strike Schwachstellen innerhalb des Betriebssystems ausnutzen.
- ☑ Aufzeichnung von Eingaben (T1056)/Bildschirmaufzeichnung (T1113)
- ☑ Cobalt Strike kann auch als Keylogger fungieren und Bildschirmfotos vom infizierten System sammeln.

ANTWORT

- ☑ **WO:** Unbekannt
- ☑ **WEM:** Mehrere Organisationen rund um den Globus
- ☑ **WARUM:** Cobalt Strike wurde in mehreren Kampagnen eingesetzt, die unterschiedliche Ziele verfolgten. Ein Grund für den Angriff ist es, sich Zugang zum internen Unternehmensnetzwerk zu verschaffen, um sich dort zu bewegen. Ein anderer Grund könnte sein, Unternehmen Schaden zuzufügen, indem das kompromittierte Netzwerk z. B. mit einer Ransomware angegriffen wird.
- ☑ **WAS:** Hauptsächlich für den Fernzugriff, die Kompromittierung von Netzwerken und seitliche Bewegungen.
- ☑ **WIE:** Cobalt Strike ist ein kommerzielles Red-Teaming-Tool, mit dem gekaperte Cyberangriffe simuliert werden können. Das Tool wird verwendet, um den anfänglichen Zugang zu einem Unternehmensnetzwerk zu erlangen sowie für weitere Aktionen mit dem kompromittierten Netzwerk.
- ☑ **STRATEGIE:** Depending on the attacked company, the information on how they identified and reacted on the attack is unknown.

WIEDERHERSTELLEN

☑ **AUSWIRKUNG:** Der Angreifer kann sich vollen Netzwerkzugang innerhalb des Unternehmens verschaffen. Dies kann zur Offenlegung von Informationen sowie zu weiteren Angriffen führen, die je nach Betreiber des Angriffs durchgeführt werden.

☑ **WIEDERHERSTELLUNGSSTRATEGIE:** Je nach angegriffenem Unternehmen ist nicht bekannt, wie deren Wiederherstellungsstrategie aussieht.

BESSERE STRATEGIE:

- Antivirensysteme auf dem neuesten Stand halten
- Intrusion Detection- und Intrusion Prevention-Systeme verwenden
- Ordnungsgemäße Überwachung der Systeme auf verdächtige Aktivitäten
- Systeme ordnungsgemäß konfigurieren und nicht benötigte Dienste deaktivieren
- Schulung des Bewusstseins der Mitarbeiter
- Segmentierung auf Netzwerkebene und Beschränkung der erlaubten Kommunikation auf ein erforderliches Minimum

LESSONS LEARNT

Obwohl es notwendig ist, Red-Teaming-Tools zu entwickeln, die für die Simulation von Angriffen auf ein Netzwerk verwendet werden können, um mögliche Schwachstellen zu finden, muss man dennoch bedenken, dass ein solches Tool auch kompromittiert und von einem Angreifer verwendet werden kann.

FALLSTUDIE 8: ZERO-DAY-ANGRIFF - HACKERGRUPPE HAFNIUM NIMMT EXCHANGE-SERVER INS VISIER

BETROFFENE ORGANISATION

Anfang 2021 fanden Forscher mehrere kritische Schwachstellen im Microsoft Exchange Server, die weltweit massiv ausgenutzt wurden. Die Schwachstellen wurden von mehreren kriminellen Organisationen, vor allem der HAFNIUM-Gruppe, ausgenutzt, bevor Microsoft Patches zur Verfügung stellte. Dies machte es besonders schwer, auf die Angriffe zu reagieren und sich von ihnen zu erholen.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Methode, die zur Sammlung der Informationen für diese Fallstudie angewandt wurde, war Desk Research; die spezifischen Informationsquellen sind im Abschnitt Referenzen dieses Dokuments zu finden.

VORBEUGEN

Zehntausende von Unternehmen waren von diesem Angriff betroffen. Da Microsoft Exchange Server generell dem Internet ausgesetzt sind und die Authentifizierung umgangen werden kann, war der Angriff von vornherein nur sehr schwer zu verhindern. Dies legt die Vermutung nahe, dass die verschiedenen Sicherheitspraktiken, die für diese Unternehmen gelten, keinerlei Auswirkungen hatten.

IDENTIFIZIEREN

Es gibt vier verschiedene Sicherheitslücken, die zu den beschriebenen Angriffen führten. Die Schwachstellen sind **CVE-2021-26855, bekannt als "ProxyLogon", CVE-2021-27065, CVE-2021-26857 und CVE-2021-26858.** Die Technik zur Ausnutzung dieser Schwachstellen wird als **"Exploitation for Client Execution**" (T1203) im MITRE ATT&CK-Framework beschrieben.

CVE-2021-26855 ist eine Umgehung der Authentifizierung über den internen Proxy des Exchange Servers. Damit kann ein Angreifer privilegierten Zugriff auf den Server selbst erhalten. Die Kombination mit einer anderen Schwachstelle wie CVE-2021-27065, die das Schreiben beliebiger Dateien auf das System ermöglicht, oder CVE-2021-26857, mit

der über eine unsichere Deserialisierung SYSTEM-Zugriff (T1078) erlangt werden kann, schafft eine uneingeschränkte Ausnutzungskette.

Die Angriffe fanden in freier Wildbahn statt, bevor Microsoft einen Patch für die Sicherheitslücken veröffentlichen konnte. Nach Angaben zahlreicher Quellen betrug die Zeitspanne der Zero-Day-Exploitation rund 58 Tage. Die erste Gruppe, die mit diesen Sicherheitslücken in Verbindung gebracht wurde, war HAFNIUM. Später begannen mehrere andere Gruppen, diese Sicherheitslücken auszunutzen. Die Fähigkeiten des Angriffs ermöglichten mehrere Szenarien, die von der Datenexfiltration (T1567) bis zum Einsatz von Ransomware (T1486) reichten.
Es folgt eine Liste der Aktionen, die die HAFNIUM-Gruppe mit diesem Angriffsvektor durchgeführt hat:

- ☑ T1589 – Sammeln von E-Mail-Adressen von Nutzern, die sie ansprechen wollten
- ☑ T1071 – Open-Source-C2-Framework (z. B. Covenant)
- ☑ T1560 - 7-Zip, WinRAR zum Komprimieren gestohlener Dateien für die Extraktion
- ☑ T1059 - Exportieren von Mailboxdaten über PowerShellT1567 – Exfiltrate data via sharing sites, including MEGA
- ☑ T1105 - Herunterladen von Malware und Tools auf kompromittierte Hosts (z. B. Nishang, PowerCat)
- ☑ T1003 - Credential Dumping von LSASS- und Active Directory-Datenbanken (NTDS.DIT)
- ☑ T1505 - Bereitstellung von WebShells auf kompromittierten Hosts (SIMPLESEESHARP, SPORTSBALL, usw.)

Phishing ist ein Sammelbegriff für Social-Engineering-Angriffe, die derzeit über E-Mails oder Anwendungen in sozialen Netzwerken durchgeführt werden.

Die Identifizierung der Angriffe kann durch die Überprüfung von Protokollen auf möglicherweise kompromittierten Rechnern erfolgen. Microsoft veröffentlichte den Guide “ guidance on detecting every vulnerability according to their Indicator of Compromise.”

ANTWORT

WO: HAFNIUM (wahrscheinlich staatlich geförderte Gruppe mit Verbindungen zu China)
WHOM: Verschiedene Unternehmen rund um den Globus, hauptsächlich US-Industrie
WARUM: Datenexfiltration und wahrscheinlich Geld verdienen über Ransomware
WAS: Firmenwissen wie Daten, E-Mail-Adressen, Postfächer
WIE: Ausnutzung mehrerer Sicherheitslücken in Microsoft Exchange Server, um nicht autorisierte Remotecodeausführung zu ermöglichen
STRATEGIE: Scannen des IP-Bereichs im Internet, um IP-Listen von Microsoft Exchange-Servern zu sammeln. Ausnutzung der genannten

Schwachstellen zur Bereitstellung von Web-Shells oder C2-Beacons. Nutzung dieses Zugangs, um Daten zu komprimieren und über Online-Sharing-Websites wie MEGA zu exfiltrieren. Gelegentlicher Einsatz der Ransomware "DearCry". Dies war aufgrund der späten Verfügbarkeit des Patches und des schlechten Patch-Managements der Unternehmen möglich.

WIEDERHERSTELLEN

AUSWIRKUNG: Die Folgen dieses Angriffs können als Informationsverlust betrachtet werden, da sowohl die Exfiltration als auch die Ransomware in diese Kategorie fallen. Wenn Unternehmen versucht haben, das Lösegeld zu zahlen, um ihre Daten zurückzubekommen, haben sie außerdem einen finanziellen Schaden erlitten.

WIEDERHERSTELLUNGSSRATEGIE: Je nach Art des Angriffs kann die Wiederherstellung unterschiedlich ausfallen. Der Wiederherstellungsprozess nach einem Ransomware-Angriff kann lange dauern. Alle infizierten Systeme müssen entweder neu installiert werden oder es muss ein Backup wiederhergestellt werden. Wenn Backups auf einem infizierten System gespeichert wurden, können sie natürlich nicht für den Wiederherstellungsprozess verwendet werden.
Die Wiederherstellung nach einer Datenexfiltration ist anders. Zunächst sollten verfügbare Patches angewendet und Spuren von Web-Shells oder C2-Beacons entfernt werden. Es ist wichtig zu bewerten, welche und wie viele Daten gestohlen wurden, um die Auswirkungen zu messen.

BESSERE STRATEGIE

- ☑ Antivrussystem aktuell halten
- ☑ Intrusion Detection und Intrusion Prevention Systeme verwenden
- ☑ Ordnungsgemäße Überwachung von Systemen auf verdächtige Aktivitäten
- ☑ Ordnungsgemäße Konfiguration von Systemen und Deaktivierung nicht benötigter Dienste
- ☑ Schnelles Patch-Management, um Schwachstellen so schnell wie möglich zu beheben
- ☑ Segmentierung auf Netzwerkebene und Beschränkung der erlaubten Kommunikation auf ein erforderliches Minimum

LESSONS LEARNT

Zero-Day-Exploitation mit Angriffsketten wirkt sehr einschüchternd. Der Schlüssel zur Bewältigung dieser Herausforderungen ist eine angemessene Netzwerksegmentierung und Systemüberwachung, um mögliche Angriffe rechtzeitig zu erkennen. Systeme zur Verhinderung von Eindringlingen in das Netzwerk können ebenfalls zur Erkennung solcher Angriffe beitragen.

Wichtig ist auch, dass Patches für kritische Schwachstellen so schnell wie möglich angewendet werden, um weitere Angriffsvektoren zu beseitigen.

Als weitere Lektion möchte ich die Sicherheitsforscher von DevCore erwähnen, die die Schwachstellen zuerst entdeckten und Microsoft beim Patch-Prozess halfen. Dies unterstreicht die Bedeutung unabhängiger Sicherheitsforschung für die gute Sache.

FALLSTUDIE 9: WannaCry: WENN EINE RANSOMWARE DAS GESUNDHEITSSYSTEM LAHMLEGT

BETROFFENE ORGANISATION

Im Jahr 2017 infizierte eine neue Ransomware namens **WannaCry (WannaCrypt**), die auf das Windows-Betriebssystem abzielt, Abertausende von Kunden auf der ganzen Welt. Der Angriff richtete sich nicht gegen eine bestimmte Organisation, sondern war weit verbreitet und betraf viele Unternehmen in verschiedenen Bereichen.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Methode, die zur Sammlung der Informationen für diese Fallstudie angewandt wurde, war Desk Research; die spezifischen Informationsquellen sind im Abschnitt Referenzen dieses Dokuments zu finden.

VORBEUGEN

Mehrere Unternehmen waren von diesem Angriff betroffen, was die Vermutung nahe legt, dass die unterschiedlichen Sicherheitspraktiken, die für diese Unternehmen gelten, keinerlei Auswirkungen hatten.

IDENTIFIZIEREN

WannaCry ist eine bösartige Anwendung, die als **Ransomware** eingestuft wird, da sie benutzerspezifische Dateien auf einem Zielsystem verschlüsselt. Dies führt zur Manipulation von Daten und deren Zerstörung, da der Besitzer des infizierten Systems nicht in der Lage ist, die Dateien zu entschlüsseln. Dies führt zu einem Denial-of-Service-Angriff aufgrund der fehlenden Dateien und Daten.

Eines der Hauptmerkmale von WannaCry ist die Technik, mit der automatisch nach potenziellen Zielsystemen gesucht wird, die die Ransomware dann ebenfalls zu infizieren versucht. Da diese Malware andere Systeme von einem bereits infizierten System aus infizieren kann, wird sie auch als Wurm bezeichnet. Um dieses Ziel zu erreichen, wird ein Exploit für eine Software-Schwachstelle im SMB-Protokoll von Microsoft Windows namens Eternal Blue verwendet, das der MITRE ATT&CK ID T1210 zugeordnet ist.

Bevor sich die Malware ausbreiten und andere Systeme infizieren kann, muss sie diese zunächst suchen und finden. Dies geschieht über verschiedene Techniken wie das Scannen nach entfernten Systemen (T1018), das Aufzählen aktiver Remote-Desktop-Sitzungen (T1563) und das Scannen nach neuen angeschlossenen Laufwerken auf dem infizierten System (T1120). Sobald ein potenzielles

Remote-Gerät oder -Laufwerk gefunden wurde, versucht WannaCry, sich auf das Zielsystem zu kopieren und sein bösartiges Verhalten auszuführen.

Bevor die Ransomware mit der Verschlüsselung beginnt, nimmt sie Änderungen am infizierten System vor, um die Wiederherstellungsoptionen zu deaktivieren (T1490). Anschließend sucht sie in Verzeichnissen nach benutzerspezifischen Dateien (T1083) und beginnt mit der Verschlüsselung jeder gefundenen Datei (T1486).

Für eine verhaltensbasierte Identifizierung dieses Angriffs können die folgenden MITRE ATT&CK-Techniken verwendet werden:

- ☑ T1210: Exploitation of Remote Services
- ☑ T1018: Remote System Discovery
- ☑ T1563: Remote Service Session Hijacking (.002 RDP Hijacking)
- ☑ T1120: Peripheral Device Discovery
- ☑ T1490: Inhibit System Recovery
- ☑ T1083: File and Directory Discovery
- ☑ T1486: Data Encrypted for Impact
- ☑ T1573: Encrypted Channel (.002 Asymmetric Cryptography)
- ☑ T1090: Proxy (.003 Multi-hop Proxy)

"Der WannaCry-Ausbruch hat über 200.000 Computer in über 150 Ländern befallen. Er kostete das Vereinigte Königreich 92 Millionen Pfund und verursachte weltweit Kosten in Höhe von bis zu 6 Milliarden Pfund." (Acronis, 2020)

ANTWORT

Im Jahr 2017 infizierte eine neue Ransomware namens WannaCry (WannaCrypt), die auf das Windows-Betriebssystem abzielt, Abertausende von Kunden auf der ganzen Welt. Der Angriff richtete sich nicht gegen eine bestimmte Organisation, sondern war weit verbreitet. Große Unternehmen, von denen einige ihre Geschäfte weltweit betreiben, wie z. B. Automobilhersteller, waren von der Ransomware betroffen. Aber auch andere Organisationsgruppen wie öffentliche Verkehrsmittel, Gesundheitsdienste oder Telekommunikationsdienste waren betroffen.

- ☑ **WER:** Unbekannt
- ☑ **WEM:** Different companies around the globe
- ☑ **WARUM:** Erreichnung eines hohen Schaden durch Datenverlust und Erpressungsgeld
- ☑ **WAS:** Unternehmenswissen wie Daten
- ☑ **WIE:** Infektion mit Ransomware, die über eine in Microsoft Windows gefundene Sicherheitslücke verbreitet wurde
- ☑ **STRATEGIE:** Die von WannaCry verwendete Lösegeldforderung erschien auf dem Bildschirm der infizierten Systeme. Antivirensysteme und Firewalls erkannten die Infektion und Verbreitung der Ransomware und konnten die Systeme daher nicht vor weiteren Infektionen und Schäden schützen.

WIEDERHERSTELLEN

IMPACT: Die Folgen dieses Angriffs können als Informationsverlust angesehen werden, da alle Dateien, die von der Ransomware verschlüsselt wurden, nicht mehr lesbar sind. Wenn Unternehmen versucht haben, das Lösegeld zu zahlen, um ihre Daten zurückzubekommen, haben sie außerdem einen finanziellen Schaden erlitten.

WIEDERHERSTELLUNGSSTRATEGIE: Der Wiederherstellungsprozess nach einer Ransomware kann lange dauern. Alle infizierten Systeme müssen entweder neu installiert werden oder es muss ein Backup wiederhergestellt werden. Wenn Backups auf einem infizierten System gespeichert wurden, können sie natürlich nicht für den Wiederherstellungsprozess verwendet werden.

BESSERE STRATEGIE

- ☑ Antivirensysteme auf dem neuesten Stand halten
- ☑ Intrusion Detection- und Intrusion Prevention-Systeme verwenden
- ☑ Monitoringsystem
- ☑ Professionelle Konfiguration, Deaktivierung nicht benötigter Dienste
- ☑ Schnelles Patch-Management
- ☑ Training Bewußtsein der MitarbeiterInnen
- ☑ Segmentierung auf Netzwerkebene und Beschränkung der erlaubten Kommunikation auf ein erforderliches Minimum

LESSONS LEARNT

Ransomware-Angriffe sind heutzutage weit verbreitet und können alle Unternehmen treffen. Es wird dringend empfohlen, bekannte Sicherheitspraktiken zu befolgen, um die IT-Infrastruktur so sicher wie möglich zu machen und den Schaden eines Angriffs so gering wie möglich zu halten.

FALLSTUDIE 10: SENSIBLE PRIVATE DATEN AUSSPIONIEREN

Betroffene ORGANISATION

Im Herbst 2020 wurde auf nationaler Ebene eine neue Sicherheitswarnung veröffentlicht. Darin wurde darauf hingewiesen, dass viele öffentliche und private Einrichtungen, ähnlich wie bei anderen aufeinanderfolgenden Wellen, von Malware-Angriffen des Typs EMOTET schwer betroffen waren, was zu zahlreichen Problemen führte. EMOTET ist eine Malware, die Computer, auf denen das Betriebssystem Microsoft Windows läuft, über infizierte bösartige Links oder Anhänge (z. B. PDF, DOC, ZIP usw.) infiziert.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die zur Beschreibung dieses Cyberangriffs benötigten Informationen wurden durch ein Interview mit einem IT-Techniker des Unternehmens gesammelt. Das Gespräch wurde unter der Bedingung geführt, dass sensible Informationen anonym bleiben. Auch wenn der Befragte bereit war, den Vorfall zu beschreiben, konnten einige Informationen nicht eingeholt werden, da das Problem an ein spezialisiertes Unternehmen delegiert wurde und separat untersucht werden musste.

Vorbeugen

Obwohl spezialisierte Einrichtungen und Organisationen Kampagnen zur Sensibilisierung für die zu ergreifenden Maßnahmen durchgeführt haben, waren laut den vorliegenden Berichten viele öffentliche und private Organisationen betroffen.

Im Fall des untersuchten Unternehmens gab es im Hinblick auf die Cybersicherheit spezifische Verfahren und Mechanismen, die jedoch aufgrund der geringen Erfahrung einiger Mitarbeiter auf dem Gebiet der digitalen Domäne nicht ausreichend waren.

IDENTIFIZIEREN

Emotet ist ein Trojaner, der ursprünglich mit Bankbetrug in Verbindung gebracht wurde und sich seit 2017 auf die Verbreitung von Spam und sekundären Nutzdaten beschränkt. Derzeit können zahlreiche Varianten von Emotet identifiziert werden, und leider entwickelt sich diese Malware weiter zu neuen Varianten mit komplexeren Fähigkeiten und Umgehungstechniken.
Auf der Grundlage der bereitgestellten Beschreibungen und ergänzend zu Medienberichten waren die folgenden Details an dem Vorfall beteiligt:

- ☑ Es wurde eine sozial konstruierte Phishing-E-Mail empfangen, an die ein gezipptes Archiv angehängt ist und in der das Kennwort enthalten ist.
- ☑ Die Malware war verschlüsselt und passwortgeschützt in einer Archivdatei
- ☑ Umgehung von Anti-Malware-Lösungen durch Verwendung passwortgeschützter Archive als Anhänge

"EMOTET war viel mehr als nur eine Malware. Was EMOTET so gefährlich machte, war, dass die Malware anderen Cyberkriminellen zur Miete angeboten wurde, um andere Arten von Malware, wie Banking-Trojaner oder Ransomware, auf dem Computer eines Opfers zu installieren." (EUROPOL, 2022)

☑ Der Trojaner-Loader enthielt gutartigen Code aus einer Microsoft-DLL, um Antivirenlösungen zu umgehen

☑ Thread-Hijacking zur Verbreitung von bösartigem Code unter Verwendung passwortgeschützter Archive als Anhänge

☑ Kompromittierte Systeme wurden genutzt, um bösartige E-Mails an andere Kontakte zu senden.

☑ E-Mail-Systeme vorübergehend abgeschaltet, um eine weitere Verbreitung des Trojaners zu verhindern

☑ Beeinträchtigte interne Netzwerke

Nach dem MITRE ATT&CK-Rahmenwerk kann dieser Vorfall wie folgt beschrieben werden:

1. T1566.001 - Spearphishing-Anhang
2. T1204.002 - Benutzer-Ausführung: Bösartige Datei
3. T1027 - Verdeckte Dateien oder Informationen
4. T1036 - Maskerade
5. T1586.002 - Kompromittierte Konten: E-Mail-Konten
6. T1586.002 - Kompromittierte Konten: E-Mail-Konten
7. T1499 - Denial of Service an Endpunkten
8. T1498 - Netzwerk-Denial-of-Service

Antworten

WER: Der Angreifer konnte nicht genau identifiziert werden. Nur der Herkunftsort, Vietnam, war bekannt.
WEM: nicht spezifisch gezielt
WARUM: Sammeln von sensiblen Daten und Auszahlung von Ransomware
WAS: Unternehmens-/Nutzerdaten
WIE: Spearphishing-Angriff, Skriptausführung, Prozessinjektion.
STRATEGIE: Die Bedrohung begann auf einem Computer ohne Antivirenprogramm und hat sich seither weiter ausgebreitet. Eine Reinigung wurde von einem auf IT&C spezialisierten Unternehmen durchgeführt.

Wiederherstellen

IMPACT: Die wichtigsten Folgen des Angriffs waren folgende:

- ☑ Datenverlust
- ☑ Unterbrechung der regelmäßigen Aktivitäten
- ☑ Gefährdung des Systems
- ☑ Finanzielle Kosten

Wiederherstellungsstrategie: Die Wiederherstellungsstrategie konzentrierte sich auf die Säuberung und Neuinstallation der

kompromittierten Computer sowie die Säuberung und/oder Neuinitialisierung der kompromittierten E-Mail-Postfächer.

BESSERE STRATEGIE

- ☑ Installieren Sie ein Antivirus-/Antimalware-Programm und halten Sie es auf dem neuesten Stan
- ☑ Netzwerk-Intrusionsschutz einführen
- ☑ Web-basierte Inhalte einschränken
- ☑ Sicherstellung der Sensibilisierung der Benutzer
- ☑ Bessere Passwortrichtlinien
- ☑ Verwaltung von privilegierten Konten
- ☑ Deaktivieren oder Entfernen von Funktionen oder Programmen
- ☑ Execution Prevention
- ☑ Audit
- ☑ User Account Management
- ☑ Verhaltensprävention am Endpunkt
- ☑ Richtlinien der Kontonutzung

LESSONS LEARNT

Auch wenn Emotet durch eine internationale konzertierte Aktion ausgeschaltet wurde, bleibt abzuwarten, ob dies langfristige Auswirkungen haben wird.

Es ist anzumerken, dass Schadprogramme fast dieselben Techniken verwenden, um in die freie Wildbahn einzudringen und sich zu verbreiten, so dass es zwingend erforderlich ist, aufmerksam und vorsichtig zu sein, da es auch in Zukunft Cyberangriffe geben wird. Maßnahmen wie die Kommunikation mit der Welt über einen Computer, der von dem Netz, in dem sich kritische Infrastrukturen befinden, isoliert ist, die Verwendung leistungsfähiger und aktueller Sicherheitslösungen und die Verwendung der neuesten Updates sind einige der Maßnahmen, die vorgesehen werden sollten..

FALLSTUDIE 11: UNERLAUBTER ZUGANG ZU ANMELDEINFORMATIONEN

Betroffene ORGANISATION

Wie jedes moderne Unternehmen ist in der beschriebenen Situation die elektronische Kommunikation über das Internet mit seinen Kunden und Lieferanten der bevorzugte Weg. Bei dieser Art der Kommunikation ist die elektronische E-Mail eine der am häufigsten verwendeten. Sie ermöglicht die asynchrone Kontaktaufnahme mit den Beteiligten, die von mehr als einer Person effizient verwaltet wird. Das Unternehmen, das seit über einem halben Jahrhundert auf dem Markt ist, hat die Digitalisierung in allen Abteilungen stark vorangetrieben, und in diesem Zusammenhang ist auch die Abteilung für Kundenbeziehungen einbezogen. Für die entsprechenden Mitarbeiter wurde eine E-Mail-Gruppe eingerichtet, die die Online-Anfragen von speziellen Computern aus verwaltet, die durch Antivirus- und Spam-Filterfunktionen auf dem E-Mail-Server geschützt sind.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die zur Beschreibung dieses Cyberangriffs benötigten Informationen wurden durch ein Interview mit einem der IT-Techniker des Unternehmens gesammelt. Das Gespräch wurde unter der Bedingung geführt, dass sensible Informationen anonym bleiben. Auch wenn der Befragte bereit war, den Vorfall zu beschreiben, konnten einige Informationen nicht eingeholt werden, da das Problem von einem anderen Team bearbeitet wurde.

VORBEUGEN

Obwohl die Nationale Direktion für Cybersicherheit Aufklärungskampagnen über die zu treffenden Maßnahmen durchgeführt hat, sind laut vorliegenden Berichten viele öffentliche und private Organisationen und Einzelpersonen betroffen.

Das Unternehmen hat die Verwendung von Sicherheitstools und benutzerdefinierten Vorschriften für die Online-Arbeit durchgesetzt, aber dies reichte aufgrund der geringen Erfahrung einiger Mitarbeiter im Bereich der digitalen Domäne nicht aus.

IDENTIFIZIEREN

Phishing ist ein Sammelbegriff für **Social-Engineering-Angriffe**, die derzeit über E-Mails oder Social-Networking-Anwendungen durchgeführt werden.

In der Regel verschicken Cyberkriminelle massenhaft unaufgeforderte Nachrichten. Sie wollen so viele Menschen wie möglich ansprechen, um einige von ihnen mit ihrem Trick zu erwischen

Cyberkriminelle versuchen, den Trend zu einer Art "tollem Angebot" oder zu administrativen Anweisungen auszunutzen. Viele dieser Arten von Nachrichten scheinen legitim zu sein, da sie die gleiche visuelle Identität wie bekannte Unternehmen, Online-Dienste oder Anwendungen verwenden. Einige Beispiele sind Unternehmen wie Google, Amazon, Microsoft, Yahoo, LinkedIn usw. oder beliebte Bankdienste und Anwendungen wie die Verwaltung webbasierter E-Mails.

Die Glaubwürdigkeit soll durch das Kopieren von Farbschema, Stil, Logo und Mottos der kopierten Identität erreicht werden. Es werden typische attraktive Betreffzeilen verwendet.

Ausgehend von der vorgelegten Beschreibung und ergänzenden Medienberichten waren die folgenden Details in den Vorfall verwickelt:

- ☑ Es wurde eine sozial konstruierte Phishing-E-Mail empfangen, in der behauptet wurde, dass das Zugangspasswort dringend geändert werden müsse, um das Ende des Dienstes zu verhindern;
- ☑ Die Weitergabe der Zugangsdaten an die unrechtmäßige Einrichtung führte zum Zugriff auf das E-Mail-Konto und zur Beendigung des rechtmäßigen Zugriffs durch Änderung des Passworts;
- ☑ Das kompromittierte Konto wurde für unerwünschte Phishing-Nachrichten verwendet, die an die vorhandenen Kontakte und andere Adressen des Angreifers gesendet wurden;
- ☑ Aufgrund massiver Spam-Nachrichten, die über das Internet verschickt wurden, wurde der E-Mail-Dienst auf eine schwarze Liste gesetzt, so dass der normale Betrieb gestört wurde;
- ☑ Das E-Mail-System wurde vorübergehend ausgesetzt, um weiteres Spamming zu verhindern;
- ☑ Der Online-Betrieb wurde beeinträchtigt.

Nach dem MITRE ATT&CK-Rahmen kann dieser Vorfall wie folgt beschrieben werden:

1. T1598.001 - Spearphishing-Dienst
2. T1598.002 - Spearphishing-Anhang
3. T1598.003 - Spearphishing-Link

Antworten

- ☑ **WER:** Der Angreifer konnte nicht genau identifiziert werden, da die Herkunft aus mehreren Ländern protokolliert wurde. Möglicherweise war eine VPN-Nutzung im Spiel.
- ☑ **WEM:** nicht spezifisch gezielt
- ☑ **WARUM:** Sammlung sensibler Daten und Erpressung von Geld
- ☑ **WAS:** Unternehmens-/Nutzerdaten
- ☑ **WIE:** Phishing, Diebstahl von Anmeldedaten.
- ☑ **STRATEGIE:** Die Bedrohung begann mit dem Öffnen einer gefälschten E-Mail, dem Zugriff auf gefälschte Links und der Übermittlung sensibler Daten. Das IT-Team setzte die Anmeldedaten zurück und strich sie aus den schwarzen Listen der Dienste.

WIEDERHERSTELLEN

IMPACT: Die wichtigsten Folgen des Angriffs waren folgende:

- ☑ Verlust von Zugangsdaten
- ☑ Unterbrechung der regelmäßigen Aktivitäten
- ☑ Systemkompromittierung.

WIEDERHERSTELLUNGSSTRATEGIE: Die Wiederherstellungsstrategie konzentrierte sich auf das Zurücksetzen der Anmeldedaten und die Bereinigung der kompromittierten E-Mail-Clients..

BESSERE STRATEGIE

- ☑ Installieren Sie ein Antivirus-/Antimalware-/E-Mail-Filtersystem und halten Sie es auf dem neuesten Stand.
- ☑ Einführung eines Systems zur Verhinderung von Netzwerkeinbrüchen
- ☑ Web-basierte Inhalte einschränken
- ☑ Sicherstellung der Sensibilisierung der Benutzer
- ☑ Bessere Passwortrichtlinien
- ☑ Verwaltung von privilegierten Konten
- ☑ Prüfung
- ☑ Verwaltung von Benutzerkonten
- ☑ Verhaltensprävention am Endpunkt
- ☑ Richtlinien für die Kontonutzung.

LESSONS LEARNT

Auch wenn Phishing keine neue Technik ist, so bleibt es doch eine der Hauptmethoden bei vielen Cybersicherheitsangriffen.

Es ist anzumerken, dass Schadsoftware fast ausschließlich diese Technik nutzt, um in die freie Wildbahn einzudringen und sich zu verbreiten, so dass es zwingend erforderlich ist, sich dessen bewusst zu sein und vorsichtig zu sein, da es auch weiterhin Cyberangriffe dieser Art geben wird. Maßnahmen wie die Verwendung besserer, aktualisierter und geschützter E-Mail-Dienste, ein stärkeres Bewusstsein für den Zugriff auf E-Mails und eine gründliche Analyse der Legitimität des Absenders.

FALLSTUDIE 12: VERALTETE, EXPONIERTE ONLINE-ANWENDUNGEN

BETROFFENE ORGANISATION

Heutzutage haben viele Unternehmen die Art und Weise, wie sie ihre Dienstleistungen erbringen, geändert, indem sie online gehen. Dies ist der Fall bei dem Beispiel eines stillgelegten Unternehmens, das 1998 mit der Erbringung von Finanzdienstleistungen am Schreibtisch begann und seit mehr als einem Jahrzehnt online ist. Der neue Ansatz verbesserte die Gesamttätigkeit des Unternehmens und die Zufriedenheit der Kunden. Diese Errungenschaften waren jedoch nur nach erheblichen Anstrengungen bei der Entwicklung der erforderlichen, eigens entwickelten Software möglich. Diese Online-Anwendung ermöglichte es den Kunden und den Mitarbeitern, die erforderlichen Vorgänge durchzuführen. Die zur Verfügung gestellte Plattform, die in dieser Zeit entwickelt wurde, wurde so lange beibehalten, bis der Support vor der Veröffentlichung des neuen großen Upgrades verfügbar war. Im Laufe der Zeit wurde die Anzahl der Mitarbeiter aufgrund der Automatisierung der bestehenden Prozesse und der Marktveränderungen reduziert. Das Upgrade auf die neue Distribution verzögerte sich, da umfangreiche Hardware und Software erforderlich waren.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Informationen, die zur Beschreibung dieses Cyberangriffs benötigt werden, wurden durch ein Interview mit dem Geschäftsführer des Unternehmens gesammelt. Das Gespräch wurde unter der Bedingung geführt, dass die sensiblen Informationen anonym bleiben..

VORBEUGEN

Obwohl die Nationale Direktion für Cybersicherheit Aufklärungskampagnen über die zu ergreifenden Maßnahmen durchgeführt hat, ignorieren oder verzögern viele öffentliche oder private Organisationen die für die Aktualisierung ihrer Informationssysteme erforderlichen Entscheidungen und Maßnahmen.

Das Unternehmen hat die Verwendung bekannter Sicherheitslösungen, Firewalls, Netzwerksegmentierung usw. durchgesetzt, aber diese waren nicht ausreichend, da eine Schwachstelle in einem der betriebenen Softwaremodule bestehen blieb.

Das Unternehmen hat die Verwendung bekannter Sicherheitslösungen, Firewalls, Netzwerksegmentierung usw. durchgesetzt, aber diese waren nicht ausreichend, da eine Schwachstelle in einem der betriebenen Softwaremodule bestehen blieb.

IDENTIFIZIEREN

Stream-Injection-Angriffe missbrauchen die Fähigkeit einer Online-Webanwendung, hochgeladene Inhalte wie verschiedene Arten von Dokumenten oder Bilddateien zu akzeptieren. Mit dem Ansatz der Remote-Dateieinbindung kann ein Angreifer die Schwachstelle im serverseitigen Code ausnutzen, um eine URL auf einer anderen Website als gültige Eingabe zu akzeptieren. Diese Aktion wird dann zur Ausführung von bösartigem Code des Angreifers verwendet. Außerdem kann die lokale Dateieinbindung genutzt werden, um eine Webanwendung dazu zu bringen, den gewünschten Inhalt aus dem lokalen Dateisystem zurückzugeben.

Ein bekanntes Beispiel ist das von WordPress verwendete PHP-Framework, das dem Hacker den Zugriff auf seine Konfigurationsdatei ermöglicht. Dieser Angriff kann auch den Zugriff auf alle PHP-Quellcodedateien ermöglichen, auf denen die Website läuft, was neue Möglichkeiten für andere Sicherheitslücken bietet. Neuere PHP-Versionen sind standardmäßig vor Remote File Inclusion geschützt, aber wenn versehentlich eine lokale Datei eingeschlossen wird, ist diese Art von Angriff immer noch möglich.

Ausgehend von der vorgelegten Beschreibung, ergänzenden technischen Berichten, Sicherheits- und Schwachstellen-Bulletins waren die folgenden Details von dem Vorfall betroffen:

- ☑ Durch einen Brute-Force-Angriff wird auf ein mit einem schwachen Passwort geschütztes Konto unrechtmäßig zugegriffen;
- ☑ Die entdeckten Anmeldeinformationen ermöglichen es, die mit dem Konto verbundenen Daten zu ändern;
- ☑ Durch das kompromittierte Konto konnte die Stream-Injection-Schwachstelle aufgedeckt und unerwünschter Code auf dem Server ausgeführt werden, um die Zugriffsverlaufsprotokolle zu entfernen;
- ☑ Aufgrund der unkontrollierten serverseitigen Codeausführung wurden einige Module der App unbrauchbar und führten zum Herunterfahren des Dienstes, so dass der normale Betrieb unterbrochen wurde;
- ☑ Das System wurde für weitere Untersuchungen im Zusammenhang mit der Fehlfunktion der Webanwendung vorübergehend vom Internet getrennt;

☑ Der Online-Betrieb war beeinträchtigt.

Nach dem MITRE ATT&CK-Rahmenwerk kann dieser Vorfall wie folgt beschrieben werden:

1. T1110.001 - Passwort-Raten
2. T1078 - Zugang zu gültigen Konten
3. T1518 - Entdeckung von Software
4. T1082 - Erkennung von Systeminformationen
5. T1007 - Erkennung von Systemdiensten
6. T0826 - Verlust der Verfügbarkeit.

ANTWORTEN

☑ **WER:** Der Angreifer konnte nicht genau identifiziert werden.
☑ **WEM:** keine spezielle Zielgruppe
☑ **WARUM:** Sammeln sensibler Daten und Denial-of-Service
☑ **WAS:** Unternehmens-/Nutzerdaten
☑ **WIE:** Brute-Force-Angriff, Diebstahl von Anmeldedaten und Codeausführung durch Stream-Injection.
☑ **STRATEGIE:** Die Bedrohung begann mit einem Brute-Force-Angriff, der zur Entdeckung schwacher Anmeldeinformationen, zur Ausnutzung einer Schwachstelle in einem nicht öffentlich zugänglichen Softwaremodul und anschließend zur unbefugten Codeausführung führte. Eine schwache Strategie für den Online-Zugriffsschutz, ein veraltetes Softwaremodul und ein nicht gewarteter Code sind die Hauptursachen für den Vorfall.

WIEDERHERSTELLEN

IMPACT: Die wichtigsten Folgen des Angriffs waren folgende:
☑ Verlust des Ausweises
☑ Gefährdung des Systems
☑ Regelmäßige Unterbrechung der Tätigkeit.

WIEDERHERSTELLUNGSSTRATEGIE: Die Wiederherstellungsstrategie konzentrierte sich auf ein großes Plattform-Upgrade, bei dem ein wichtiger Teil des Codes neu geschrieben wurde.

BESSERE STRATEGIE
☑ Installieren Sie eine aktuelle Software und halten Sie sie auf dem neuesten Stand.
☑ EDurchsetzung von Richtlinien für sichere Passwörter
☑ Richtlinien für die Kontonutzung
☑ Einführung eines Zwei-Faktor-Authentifizierungsmechanismus
☑ Netzwerk-Intrusionsschutz einführen
☑ Fernzugriff einschränken
☑ Sicherstellung des Benutzerbewusstseins
☑ Sicherstellung des Benutzerbewusstseins

☑ Verwaltung von Benutzerkonten
☑ Verhaltensprävention am Endpunkt.

LESSONS LEARNT

Auch wenn veraltete Software bekanntermaßen anfällig für Sicherheitslücken ist, bleibt sie doch eine der Hauptursachen für viele Angriffe auf die Cybersicherheit.

Weltweit zugängliche Webanwendungen sind vielen Schwachstellen ausgesetzt und erfordern daher in vielerlei Hinsicht besondere Aufmerksamkeit.

Maßnahmen wie die ständige Aktualisierung der Software, Verbesserungen und die Einführung neuer Techniken und Lösungen für Authentifizierungsmechanismen sowie die Einführung eines regelmäßigen Audit-Prozesses sind einige der üblichen Maßnahmen, die in Betracht gezogen werden können.

FALLSTUDIE 13: DIE RISIKEN EINES ANGRIFFS DURCH EINEN EHEMALIGEN MITARBEITER

BETROFFENE ORGANISATION

Das Unternehmen, bei dem der Cyberangriff stattfand, ist in einer Automobilbranche mit etwa 2000 Mitarbeitern tätig. Das Unternehmen befindet sich in den Bundesstaaten Paraná und Santa Catarina in Brasilien.

Der Cyberangriff zielte auf den Bereich der Informationstechnologie ab, da der Hacker als ehemaliger Angestellter des Unternehmens über Kenntnisse verfügte, die es ihm ermöglichten, das System zu überzeugen.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Informationen in dieser Fallstudie beruhen auf einer Fallstudie über die Risiken eines Cyberangriffs, der von einem ehemaligen Mitarbeiter durchgeführt wurde. Die Fallstudie wird aus der Sicht der Organisation durchgeführt, die Opfer des Cyberangriffs wurde.

Das allgemeine Ziel dieser Fallstudie ist es, die Bedeutung aufzuzeigen, die Unternehmen dem Social Engineering in ihrem Umfeld beimessen müssen, um Einbrüche und/oder Betrügereien zu vermeiden, die durch die Unachtsamkeit oder unbeabsichtigte Mithilfe von Mitarbeitern verursacht werden, um den Job des Hackers zu verletzen..

VORBEUGEN

Um möglichen Schäden vorzubeugen, verfügte das Unternehmen bereits über eine IT-Abteilung, die Firewalls, Tools für Informationsverluste und Datenverschlüsselung verwaltete.

IDENTIFIZIEREN

In dieser Fallstudie begann der Fußabdruck mit verschiedenen Besuchen auf der Webseite der Vereinigung, um ihre Dynamik, ihr Geschäft und insbesondere ihre Marken zu verstehen (da der Angreifer die Suche nach Daten lenkte, die der Hacker noch nicht kannte). Nachdem der Fußabdruck erstellt und die internen und spezifischen Informationen der Organisation auf der Seite des Angreifers sind, ging er dazu über, Verbindungen zu einer der Filialen der Kette herzustellen, um die

Namen von Managern und Personen zu ermitteln, die innerhalb der Organisation privilegierten Zugang haben könnten.

Zu diesem Zweck gab sich der Angreifer am Telefon als Kunde aus, der rechtliche Probleme mit dem Unternehmen hatte. Um dieses Problem zu lösen, hätte das Unternehmen den Kunden angerufen und ihn gebeten, mit dem Leiter der betreffenden Filiale zu sprechen, da er/sie die Person mit der größten Autonomie wäre, die in einer solchen Situation antworten könnte. Dank dieser Interaktion war es ein Leichtes, den Namen des Geschäftsführers, den Ort, an dem er/sie arbeitet, und die Telefonnummer zu erfahren.

Nach diesem Telefonat wurde versucht, den Manager auf den bekannten Wegen zu kontaktieren, um die gesammelten Informationen zu überprüfen. Das Zurücksetzen des Passworts erfolgte durch Kontaktaufnahme mit dem Bereich Informationstechnologie, wobei man sich als der Mitarbeiter selbst ausgab, um den genannten Bereich dazu zu bringen, ihm die Zugangsdaten des Nutzers mitzuteilen.

Mit ein wenig Überredungskunst und dem Argument, dass die Daten für den Vorstand von diesem Zugang abhingen, setzte der Techniker schließlich das Passwort zurück und teilte das neue Passwort telefonisch mit. Darüber hinaus konnte er davon überzeugt werden, einen VPN-Zugang (Technologie für den Fernzugriff auf die Unternehmensumgebung) einzurichten, damit der hypothetische Benutzer von außerhalb des Büros arbeiten kann.

ANTWORTEN

WER: Der Angreifer war ein ehemaliger Angestellter;
WEM: Eine Organisation, die sich mit kommerziellen Nachfolgeprojekten in der Automobilbranche beschäftigt;
WARUM: Der Angriff wurde mit unbekannten Motiven auf die Organisation gerichtet;
WAS: Das Zielobjekt war der Informationstechnologiesektor, um Insiderinformationen über das Unternehmen und persönliche Daten der derzeitigen Mitarbeiter zu sammeln;

WIE: Der Angriff begann damit, dass er den Namen des Geschäftsführers einer Filiale ausspionierte, sich dann mit der IT-Abteilung des Unternehmens in Verbindung setzte und sie überzeugte, das Passwort zurückzusetzen. Auf diese Weise gab sich der Ex-Mitarbeiter als Manager aus und hatte Zugang zu allen Insider-Informationen, persönlichen Daten von Mitarbeitern und Kunden und allem, was der Hacker sonst noch wollte..

WIEDERHERSTELLEN

Das Unternehmen begann, die Mitarbeiter zu schulen, damit sie darauf achten, welche Art von Informationen sie üblicherweise an Dritte weitergeben, insbesondere wenn es sich um kritische Informationen

handelt. Niemals, unter keinen Umständen, sollte ein Mitarbeiter kritische Informationen wie Passwörter am Telefon weitergeben. Diese müssen auf sicherem Wege an Interessenten weitergegeben werden, z. B. per Einschreiben oder über den zuständigen Vorgesetzten.

Führen Sie auch Schulungen durch, um die Mitarbeiter zu sensibilisieren, mit den Informationen, die sie im Internet weitergeben, vorsichtig umzugehen. Die Schulung konzentriert sich auf die Risiken, die die geteilten Informationen für den Beruf, aber auch für das Privatleben mit sich bringen können, wie z. B. Entführungen, Lebensdaten und persönliche Sicherheit.

Das Unternehmen ist sich bewusst, dass es die technischen und physischen Voraussetzungen für die Anwendung guter Sicherheitspraktiken schaffen muss, vor allem aber muss es die Übernahme bewährter Praktiken und strengerer Sicherheitsprotokolle durch seine Mitarbeiter wertschätzen und fördern, sei es in einem Unternehmens- oder Privatumfeld, um den schwächsten Faktor der Informationssicherheit bestmöglich zu kontrollieren: den menschlichen Faktor.

LESSONS LEARNT

Die Organisation sollte die Informationen in einem einfachen Musterverfahren erstellen, das den Hacker frustrieren kann. Dieses Verfahren hat 3 Stufen:

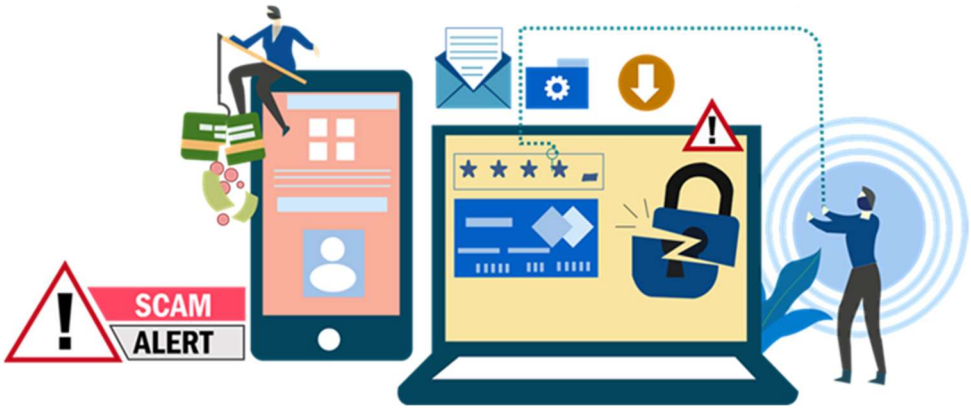
☑ **Öffentlich:** Informationen, die an jedermann weitergegeben werden können, z. B. an Geschäftskontakte und bestimmte Unternehmen, Informationen zwischen Kunden und dem Unternehmen selbst;

☑ **Privat:** Informationen, die nicht an andere Personen weitergegeben werden dürfen und die nur das Unternehmensumfeld betreffen. In diese Kategorie fallen Informationen, die sich auf interne Verfahren, Unternehmensdaten, administrative und strategische Aspekte des Unternehmens beziehen;

☑ **Vertraulich:** Informationen und Daten, die nicht innerhalb und außerhalb des Unternehmens weitergegeben werden sollten, wie z. B. Daten zur Registrierung von Mitarbeitern, Vergütungen, Ergebnisse von Bereichen und strategische Maßnahmen, die nur die Leitung oder den Vorsitz betreffen.

Außerdem sollten die Organisationen über interne Verfahren verfügen, die sie vor Angriffen durch Social Engineering schützen. Die Mitarbeiter müssen gut darin geschult werden, welche Verfahren sie befolgen und welche Maßnahmen sie in Situationen ergreifen müssen, in denen sich das Unternehmen angegriffen fühlt, wie z. B. die Weiterleitung des Anrufs an eine Person, die für diese Art von Situation geschult ist. Einfache

Maßnahmen können dazu führen, dass der Angriff fehlschlägt. Unmittelbar lässt sich sagen, dass eine erste Checkliste zur Bestätigung der Daten des Antragstellers dem Hacker bereits den Zugang erschweren würde. In Anbetracht der Tatsache, dass es nicht sehr schwierig ist, an personenbezogene Daten zu gelangen, könnten die Techniker ein Verfahren einführen, bei dem der Kontakt zur registrierten Telefonnummer des Mitarbeiters zurückverfolgt wird, um zu bestätigen, dass es sich tatsächlich um den betreffenden Mitarbeiter handelt



FALLSTUDIE 14: CYBERANGRIFFE ALS NEUE HERAUSFORDERUNG FÜR DIE INNERE SICHERHEIT

BETROFFENE ORGANISATION

Portugiesische Regierungsstellen (insbesondere das Ministerium für innere Verwaltung), die Sicherheitskräfte und große Unternehmen.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Informationen für diese Fallstudie wurden durch eine Sekundärforschung im Rahmen einer Masterarbeit gesammelt, bei der der Autor eine Studie und mehrere Sondierungsgespräche mit Fachleuten und Verantwortlichen der nationalen Sicherheitskräfte durchführte, um festzustellen, ob das Phänomen der Hacktivisten eine Bedrohung für die portugiesischen Sicherheitskräfte darstellt.

VORBEUGEN

Um Angriffe zu verhindern, überwacht das IT-Team, das für die Cybersicherheit in diesen Organisationen zuständig ist, zum Beispiel soziale Kanäle: IRCs (Internet Relay Chat), alle Arten von Chats, Facebooks, alles, wo man im Internet Informationen bekommen kann, sie machen auch ein Follow-up und versuchen zu sehen, ob es irgendwelche verdächtigen Aktionen gibt.

Nach dem "modus operandi", der von der Gruppe Anonymous (Portugal) definiert wurde, kündigen sie zunächst in sozialen Netzwerken (IRC und Facebook) die Aktionen an, die sie durchführen werden, und beginnen dann, untereinander zu kommunizieren. Dann nutzen sie private Chat-Kanäle, um miteinander zu kommunizieren, was zur Einrichtung des SOC (Security Operations Centre) des MIA (Ministerium für innere Verwaltung) führte, um sich auf diese Art von Angriffen vorzubereiten.

IDENTIFIZIEREN

Die Folgen dieser Angriffe waren je nach Art des Angriffs unterschiedlich. In vielen Fällen handelte es sich um einen Denial-of-Service-Angriff (DOS, DDOS), der eine Erschöpfung der System- oder Kommunikationsressourcen zur Folge hat. Außerdem gab es einige Arten von versuchten Eindringungsangriffen wie SQL Injection und Defacements. Das Fischen per E-Mail ist ebenfalls einer der häufigsten Angriffe, der manchmal zum Zugriff auf private Informationen führt.

Im November 2011 wurde ein Angriff auf die Website der nationalen Gewerkschaft für die Karriere von PSP-Chefs durchgeführt, bei dem persönliche und vertrauliche Daten (Patente, Telefonnummern und E-Mail-Adressen) von 107 PSP-Mitarbeitern offengelegt wurden.

"DDoS-Angriffe haben in den letzten Jahren stetig an Häufigkeit zugenommen. Einem Bericht von Cloudflare zufolge nahmen DDoS-Angriffe mit Lösegeldforderungen zwischen 2020 und 2021 um fast ein Drittel zu und stiegen im vierten Quartal 2021 im Vergleich zu den vorangegangenen drei Monaten um 75 % an." (Cook, 2022)

ANTWORTEN

Ein Angriff auf die Polizei für öffentliche Sicherheit wurde von der Gruppe LulzSec Portugal übernommen. Die portugiesische Gruppe Anonymous hat sich zu mehreren Angriffen auf Regierungswebsites und einschlägige Einrichtungen bekannt. Im Allgemeinen ist das Profil des Hackers jung, im Schulalter, auf der Sekundarstufe (10. bis 12. Klasse). Es kann aber auch vorkommen, dass es sich bereits um erwachsenere Personen handelt, die vielleicht weniger Kenntnisse im technischen Bereich haben, aber mit der Gesellschaft unzufrieden sind.

Diese Art des Angriffs ist für jeden Bürger möglich. Man muss nur im Internet nach Werkzeugen, Methoden und Gruppen suchen und schon kann man mitmachen. Diese Gruppen von Anonymous haben zur Zeit der Angriffe Workshops zur Durchführung von Angriffen durchgeführt, "ABC"-Kurse zum Verständnis von Angriffen. Sie stellen bereits entwickelte Tools zur Verfügung, auf die jeder zugreifen kann, es muss nur die Zieladresse eingegeben werden und eine Anwendung entwickelt den Angriff.

Die meisten Angreifer, d. h. junge Menschen, die noch zur Schule gehen, verwenden Tools, die von vielen Spezialisten verwendet werden, diese Spezialisten sind Menschen mit einem fortgeschrittenen akademischen Abschluss, und ältere, die bereits für den Zweck von Cyberangriffen entwickelte Tools verwenden. Das heißt, im Internet ist es möglich, Informationen zur Durchführung eines Angriffs zu suchen und zu erhalten, wie man ihn durchführt und welche Art von Werkzeugen zur Durchführung des Angriffs verwendet werden.

Der Angriff von LulzSec Portugal wurde auf Twitter damit gerechtfertigt, dass er eine Reaktion auf die Aktion von Provokateuren war, die eine von ihnen organisierte Demonstration infiltrierten.

Meistens geschehen diese Angriffe jedoch, weil diese Leute nach Sichtbarkeit streben oder die Organisationen gefährden wollen, da dies oft mit der Unzufriedenheit der Menschen in Bezug auf den aktuellen Kontext, in dem die portugiesischen Bürgerinnen und Bürger leben, zu tun hat, und die Menschen zeigen ihren Unmut oft auf diese Weise. In anderen Fällen ist es für die Angreifer im Alter von 16 oder 17 Jahren, die in sozialer Hinsicht nicht viel zu befürchten haben, nur ein Scherz, oft weil Freunde es tun und um sich in der Gruppe der Freunde zu profilieren. Meistens sind sie sich der Auswirkungen, die diese Angriffe haben können, nicht bewusst.

Alles beginnt mit einer Gruppe von Hackern, die über das technische Wissen verfügen und Tools entwickeln, die von Gruppen verwendet werden können, die nicht über das gleiche Wissen verfügen, was den Prozess des Hackens für jeden einfach macht.

Ein Merkmal der portugiesischen Gruppen ist es, ungeschützte Websites anzugreifen und Schwachstellen auszunutzen. Sie planen Angriffe über IRC (Internet Relay Chat) und Chatrooms, nehmen nicht Ihre Identität an und verwenden Nicknames. Die portugiesischen Hacktivisten verwenden die online verfügbaren Tools, um ihre Angriffe auszuführen, d. h. sie stellen keine eigenen Programme her, sondern verwenden die im Netz verfügbaren". Bei den Personen, die die Organisation und Leitung dieser Art von Initiativen übernehmen, handelt es sich häufig um Personen mit geringen technischen Kenntnissen, die sich der Ankündigung und Verbreitung der zu entwickelnden Aktionen widmen, und oft "haben diejenigen, die sogar sehr spezialisierte technische Fähigkeiten haben, keine Ahnung, dass sie die kompetentesten und spezialisiertesten in der Gruppe

sind, sie denken, dass sie Leute sind, die wenig wissen und dass sie nur anderen helfen, die mehr wissen".

Die Gruppe Anonymous verwendet herkömmliche Hacking-Methoden wie Havij114 und SQL-Injection, wobei ihre wichtigste Neuerung in der Erstellung von Websites besteht, die DoS-Angriffe durchführen.

WIEDERHERSTELLEN

Die möglichen Folgen sind der Diebstahl von Informationen, die Nichtverfügbarkeit von Diensten und die Verunstaltung von Websites, bei der Informationen verändert werden, da Hacker manchmal Informationen entfernen, aber auch hinzufügen können.

Diese Angriffe können das Vertrauen der Bürger in die Institutionen, die Opfer dieser Gruppen sind, gefährden, aber auch die Identifizierung von Schwachstellen und die Beeinflussung durch andere Personen mit bestimmten Idealen sind Situationen, die eintreten können.

Diese Arten von Angriffen entwickeln sich weiter, und die Techniken werden mit der Zeit immer besser, so dass sich die Organisationen anpassen und weiterentwickeln müssen, um ihr Netzwerk zu schützen. Sie waren gezwungen, den Zugriff auf das Netzwerk zu stoppen, bis die Bedingungen erfüllt waren, um die Sicherheit der internen Informationen zu gewährleisten. Und das haben sie bereits getan, insgesamt höchstens eine Stunde lang. Gelegentlich waren einige Dienste auch in der Nacht nicht zugänglich.

Das CNCseg (Nationales Zentrum für Cybersicherheit) befindet sich im Aufbau und wird sich mehr mit der Frage der nationalen Verteidigung befassen als das Cyberverteidigungszentrum, das in den Zuständigkeitsbereich des Verteidigungsministeriums fällt und dessen Hauptaufgabe darin besteht, Hacker anzugreifen, die möglicherweise Angriffe entwickeln, und diese Elemente aufzuspüren und zu bekämpfen.

MIA wird sich zumindest am CNCseg beteiligen und mit der GNS zusammenarbeiten, die über diese Kompetenz verfügt und eine der Informationsquellen für diese Art von Cybersicherheit sein wird. Die Idee ist, dass dieses Zentrum über Informationen über die Geschehnisse auf nationaler Ebene verfügt, das Ziel ist es, Informationen sowohl von den Technologiezentren der öffentlichen Verwaltung, dem Bankwesen, der Industrie und den verschiedenen Bereichen der portugiesischen Gesellschaft zu sammeln und damit eine Vorstellung von den Auswirkungen und dem Ausmaß eines bestimmten Angriffs zu bekommen.

LESSONS LEARNT

Hacktivismus wird als neue Herausforderung für Institutionen angesehen, und insbesondere im Fall von Sicherheitskräften kann ein Hacktivismus-Angriff schädliche Folgen haben, die sogar die Ausführung ihrer Missionen

beeinflussen können, und wird daher als echte Bedrohung angesehen, da er sich dadurch auszeichnet, dass er den Zielen der Organisation zuwiderläuft und in der Regel materielle und/oder moralische Schäden verursacht.

Die Fähigkeit hacktivistischer Gruppen, einen Angriff auszuführen, ist in der Regel gering, da sie im Netz verfügbare Tools verwenden und in Bezug auf das Hacken nicht sehr innovativ sind, sondern bestehende Schwachstellen ausnutzen. Was die Möglichkeiten angeht, so ist jeder, der über einen Computer mit Zugang zum Netz verfügt und über ein gewisses Wissen oder die Bereitschaft verfügt, aus den im Netz verfügbaren Informationen zu lernen, in der Lage, einen Cyberangriff zu entwickeln, was für die Sicherheitskräfte besorgniserregend ist.

In Bezug auf die Computersicherheit wird oft gesagt, dass es keine absolute Sicherheit und keine 100 % sicheren Systeme gibt, und die Regierung und Portugal bilden hier keine Ausnahme. Was wir beobachten konnten, ist die Schaffung einer Reihe von Infrastrukturen, die eine Sicherheitsstruktur ermöglichen, die dieser Art von Phänomenen entsprechen und auf sie reagieren kann: die vor kurzem geschaffene CNCseg, die von der PJ eingerichtet wurde, um gegen Cyberkriminalität zu kämpfen. Die Aufklärung der Menschen ist sicherlich etwas, das alle herausfordern wird, um zu erkennen, dass wir auch neue Technologien, Internetplattformen und andere Netzwerke nutzen, die die Macht haben, die Sicherheit der Bürger zu verändern.

"Ransomware wird die Opfer bis 2031 jährlich über 265 Milliarden Dollar kosten. (Cybersecurity Ventures).

Folgen eines Hacktivistenangriffs auf die nationalen Sicherheitskräfte:

- ☑ Direkt: wirtschaftliche, soziale, politische und sicherheitspolitische Folgen.
- ☑ Indirekt: das Gefühl der Sicherheit, die soziale Deregulierung und letztlich die Souveränität des Landes, der Institutionen und der Familien

. FALLSTUDIE 15: DAS "GOLDENE ZEITALTER" DER "RANSOMWARE". WIE MAN EINEN DATENKLAU VERHINDERT UND DAMIT UMGEHT

Betroffene ORGANISATION

Die meisten portugiesischen Unternehmen befinden sich in der "Generation 3" der Cybersicherheit und die Angriffe sind in der "Generation 6". In dieser Fallstudie erfahren wir, wie man vorgeht, um Ransomware-Angriffe zu verhindern, wie sie bei der IMPRESA-Gruppe immer häufiger vorkommen.

IMPRESA ist die größte portugiesische Mediengruppe, die in drei Geschäftsbereichen - Print, Digital und Fernsehen - tätig ist.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Informationen für diese Fallstudie wurden durch einen Nachrichtenartikel über die Verhinderung von Ransomware gewonnen, der ein Interview mit Rui Duro, einem Experten für Cybersicherheit, enthält.

VORBEUGEN

Die Pandemiezeiten haben das Wachstum dieser Art von Ransomware-Angriffen begünstigt. Einerseits führt die Arbeit von zu Hause aus zu einer Verstreuung der Systeme und erhöht das Risiko. Andererseits verlagern immer mehr Anwendungen ihre Systeme in die "Cloud".

"Dies birgt mehrere Risiken", sagt Rui Duro. Die Systeme befinden sich nun "bei einem anderen Dienstleister", und es ist notwendig, "Technologie auch für die Cloud zu kaufen, weil sie an sich nicht sicher ist". Für den Fachmann war "diese Entwicklung zur 'Wolke' oft schneller als die Entwicklung des Wissens der Mitarbeiter in der Informationstechnologie".

Andererseits sind viele Unternehmen von der Raffinesse der Angriffe überholt worden. "Wir (die IMPRESA-Gruppe) befinden uns in der 6. Generation von Angriffen und die meisten Unternehmen befinden sich noch in der 3. Die Mentalität muss sich ändern, es muss ein Budget und Ressourcen geben, um sich an diese neue Realität anzupassen", erklärt Rui Duro.

IDENTIFIZIEREN

Auf den Webseiten der Gruppe erscheint eine Meldung, die derjenigen ähnelt, die SIC (portugiesischer Fernsehsender) erhalten hat: "Die internen Daten der Systeme wurden kopiert und gelöscht. 50 TB an Daten sind in unseren Händen. Kontaktieren Sie uns, wenn Sie die Daten zurückhaben wollen".

Rui Duro erklärt, dass "Ransomware in der Regel in Unternehmen auftaucht, indem sie, wie wir es nennen, eine erste 'Nutzlast' im Unternehmen platziert".

Dies geschieht auf unterschiedliche Weise, z. B. durch einen Phishing-Angriff auf ein Element des Unternehmens. In anderen Fällen "lädt" jemand im Unternehmen die Malware versehentlich herunter. Es gibt noch eine dritte Möglichkeit, wenn die Akteure ein bestimmtes Unternehmen angreifen wollen und nach Schwachstellen suchen - dies ist ein "Zielangriff".

Nachdem die erste Malware in das Unternehmen gelangt ist, lädt sie eine zweite Malware herunter, die die Ransomware ausführt. Anschließend beginnt sie mit einem "Scan", bei dem sie nach Servern und anderen Systemen sucht. Das Ziel ist es, so viel Profit wie möglich zu machen - dem Experten zufolge ist es für Kriminelle "nicht sinnvoll, einen oder zwei Computer zu verschlüsseln, die Idee ist, so viele Computer wie möglich zu verschlüsseln, und zwar vorzugsweise die wichtigen".

Die Hacker installieren die Schadsoftware dann auf so vielen Systemen wie möglich, aber sie verschlüsselt die Daten nicht sofort. Normalerweise "bleibt sie mehrere Wochen, manchmal auch länger".

Die Angreifer wissen, dass Unternehmen unter anderem durch Backups wiederhergestellt werden können - sie gehen also davon aus, dass es ein Backup gibt, und sobald dieses wiederhergestellt ist, kommt es erneut zu einer Infektion.

Wenn es zu einer Verschlüsselung kommt, setzen die Kriminellen die Unternehmen unter Druck und fordern in der Regel ein Lösegeld in bar - meist in Kryptowährungen.

ANTWORTEN

Zwei Tage nach dem Angriff der Hackergruppe "Lapsus$ Group" auf die Websites der Impresa-Gruppe waren diese immer noch nicht erreichbar.

Die portugiesische Justizpolizei bestätigte, dass sie den Fall zusammen mit dem Nationalen Zentrum für Cybersicherheit (CNCS) untersucht, da die Mediengruppe bereits weiter fortgeschritten war.

Diese Verzögerung beim Zurücksetzen der Systeme ist bei Angriffen wie diesem üblich. Laut Rui Duro, verantwortlich für Check Point Software in Portugal, "ist die Zeit, die für die Bewältigung solcher Angriffe benötigt wird, sehr unterschiedlich. Sie hängt stark von der Größe des Unternehmens, dem Angriff, der Kapazität des Unternehmens im Bereich der Informationstechnologie (IT) und der Vorbereitung des Unternehmens auf den Austausch der Systeme ab. Bei einem kleinen Unternehmen dauert es manchmal ein oder zwei Tage, bei einem großen Unternehmen kann es sogar mehrere Wochen dauern, und manchmal muss die gesamte Infrastruktur neu aufgebaut werden".

Die Ransomware-Attacke ist bereits zu einer realen und unmittelbaren Bedrohung für Unternehmen auf der ganzen Welt geworden - und Portugal ist keine Ausnahme. Nach Ansicht der Europäischen Agentur für Cybersicherheit (ENISA) hat die Pandemie ein "goldenes Zeitalter" für Cyberkriminelle eingeleitet.

Nach Angaben der Agentur gab es zwischen April 2020 und Juli 2021 einen Anstieg der registrierten Angriffe um 150 %.

In Portugal gibt es noch keine offiziellen Daten für das vergangene Jahr, aber im jährlichen internen Sicherheitsbericht für 2020 wird Ransomware bereits als "die häufigste Form der Computersabotage

identifiziert, die weiterhin hohe Fallzahlen aufweist und vor allem Institutionen der Regierung sowie kleine und mittlere Unternehmen betrifft".

Diesem Bericht zufolge haben sich die Cyberangriffe in Portugal von 2019 (754 Vorfälle) auf 2020 (1418 Vorfälle) verdoppelt. Im Bereich der Informationssicherheit, wo Ransomware-Angriffe vorherrschen, gab es 2020 etwa zehnmal mehr Vorfälle als 2019. Rui Duro, Leiter von Check Point Software in Portugal, erklärt, dass "90 bis 95 % der Fälle nicht gemeldet oder bekannt werden. Die Unternehmen retten sich durch Backups und melden die Angriffe nicht".

Laut einer Studie des von ihm geleiteten Unternehmens, das technologische Sicherheitslösungen für die größten Unternehmen der Welt entwickelt, werden portugiesische Organisationen im Durchschnitt 947 Malware-Angriffe pro Woche ausgesetzt, eine Zahl, die über dem weltweiten Durchschnitt von 870 Angriffen liegt. Etwa 90 % der bösartigen Dateien kommen per E-Mail.

Daten von Check Point Software zeigen auch, dass im Dezember 2021 mehr als 2,5 % der portugiesischen Unternehmen von Ransomware-Angriffen betroffen waren.

WIEDERHERSTELLEN

Ransomware ist eine Form von Malware (eine Kombination aus den englischen Wörtern "malicious" (bösartig) und "software" (Software)), die darauf abzielt, Server und Computerspeicherbereiche zu verschlüsseln.

In der Regel zeigen die "Hacker", die hinter dem Angriff stehen, Nachrichten an, in denen sie die Zahlung eines Betrags fordern, um das System zu entschlüsseln und es dem Besitzer zurückzugeben. Dem Cybersecurity-Experten zufolge werden die Ransomware-Angriffe immer raffinierter, und es wird immer häufiger beobachtet, dass die Piraten versuchen, "doppelt oder dreifach zu erpressen".

Bei der doppelten Erpressung "kopieren sie in der Zeit, in der die Malware auf ein Backup wartet, wichtige Daten von Datenbanken, E-Mail-Servern und Finanzservern, versuchen, nach sensiblen Daten zu suchen und exportieren riesige Mengen an Daten. Und sie sagen, dass es sich nicht lohnt, den Dienst mit Backups wiederherzustellen, weil sie die Daten als Geiseln haben".

Im Falle der dreifachen Erpressung drohen die Piraten mit den sensiblen Daten in ihrem Besitz und nehmen die Kunden und Lieferanten des Unternehmens ins Visier, wenn das Unternehmen das Lösegeld nicht zahlt.

LESSONS LEARNT

Um einen Angriff zu verhindern, muss man seine Denkweise ändern und davon ausgehen, dass er passieren wird. Für den Cybersicherheitsexperten ist dies das Wichtigste. "Ich bin seit mehr als 30 Jahren auf dem Markt und arbeite in diesem Bereich. Ich habe angefangen, als die Angriffe noch ein Witz waren, verglichen mit dem, was sie heute sind, aber auch heute noch sehe ich Entscheidungsträger, die denken, dass es noch nicht besorgniserregend ist, dass es nicht relevant ist und dass sie denken, dass es ihnen nicht passieren wird. Der erste Schritt besteht darin, diese Mentalität zu ändern. Es kann jeden treffen, erst vor kurzem hat es die EDP getroffen. Wenn es passiert, muss ich darauf vorbereitet sein".

Nehmen Sie die drei Säulen der Cybersicherheit ernst: Menschen, Prozesse und Technologie

a) Menschen

"Selbst Unternehmen, die die Cybersicherheit ernst nehmen, konzentrieren sich oft zu sehr auf die Technologie, um sich zu schützen, und vergessen dabei, dass auch die Mitarbeiter geschult werden müssen, um sich sicher zu verhalten", so der Experte.

b) Prozesse

" Es ist wichtig, einen Prozess zu haben, um sich von einer Katastrophe zu erholen, Informationen zu verwalten und zu qualifizieren, ein effektives Backup-Verfahren zu haben und über Informationsspeicher zu verfügen. Viele Unternehmen sind nicht darauf vorbereitet, und in den ersten Stunden herrscht völliges Chaos, weil sie den Wiederherstellungsprozess nicht sorgfältig vorbereitet haben", erklärt er.

c) Technologie

"Der Einsatz von Technologien, die den heutigen Gegebenheiten entsprechen. Viele Unternehmen kaufen Technologie, und ich nenne das den Kauf eines "falschen Sicherheitsgefühls" - sie kaufen Technologie, die aber nicht mehr der heutigen Realität entspricht. Die traditionelle Firewall, anstatt einen fortschrittlichen Endpunkt zu kaufen, der die Systemverschlüsselung verhindert, wird ein einfacher Endpunkt verwendet, der zwar einige Malware erkennt, aber diese Verschlüsselungen nicht verhindert".

Der Spezialist erinnert daran, dass in diesen Fällen "Panik überhaupt nicht hilft". In diesen Situationen ist es notwendig, die Behörden zu informieren und auf keinen Fall das Lösegeld zu zahlen, da dies gleichbedeutend damit ist, das Verbrechen fortzusetzen und den Kriminellen zu zeigen, dass es sich lohnt. Einer der Prozesse, den die Unternehmen im Voraus festlegen müssen, ist, wie sie sich von einem solchen Angriff erholen können, damit Ruhe einkehrt und jeder seine Rolle in diesem Prozess kennt.

FALLSTUDIE 16: MALWARE/ KEYLOGGER

BETROFFENE ORGANISATION

Ein kleines Familienunternehmen des verarbeitenden Gewerbes machte ausgiebig Gebrauch vom Online-Banking. Der Mitarbeiter der Buchhaltung meldete sich mit einer firmen- und einer benutzerspezifischen Kennung und einem Passwort beim Online-Banking-System an. Bei Transaktionen über 1.000 € mussten zwei Sicherheitsfragen beantwortet werden.

Der Eigentümer wurde darüber informiert, dass eine Überweisung in Höhe von 5.000 € von einer unbekannten Quelle veranlasst wurde. Er setzte sich mit der Bank in Verbindung und stellte fest, dass Cyberkriminelle in nur einer Woche zehn Überweisungen von den Bankkonten des Unternehmens in Höhe von insgesamt 10 000 Euro vorgenommen hatten. Wie kam es dazu? Einer der Mitarbeiter hatte eine E-Mail von einem vermeintlichen Materiallieferanten geöffnet, bei der es sich jedoch um eine bösartige E-Mail handelte, die mit Malware von einem gefälschten Konto versehen war.

Ein Keylogger ist eine Software, die unbemerkt die Tastenanschläge auf dem Computer überwacht und die Informationen an einen Cyber-Kriminellen sendet.

Den Angreifern gelang es, Malware auf den Computern des Unternehmens zu installieren und mit Hilfe eines Keyloggers die Bankdaten zu erfassen. Bei einem Keylogger handelt es sich um eine Software, die unbemerkt die Tastenanschläge auf dem Computer überwacht und die Informationen an einen Cyberkriminellen sendet. Diese können dann mit gültigen Kontonummern und Passwörtern online auf Bank- und andere Finanzdienstleistungen zugreifen.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Informationen zu diesem Cyberangriff wurden durch zwei Interviews gesammelt, eines mit dem Eigentümer des Unternehmens und eines mit einem Techniker des IT-Supportunternehmens. Beide waren bereit, den Vorfall zu beschreiben und Einzelheiten zu nennen, baten aber darum, beide Unternehmen anonym zu halten, da die Informationen für sie zu sensibel waren.

VORBEUGEN

In dem untersuchten Unternehmen wurden die Verfahren und Mechanismen der Cybersicherheit als nicht zufriedenstellend eingestuft. Obwohl die Computer des Unternehmens mit Antiviren-Software ausgestattet waren, wurde keine aktualisiert. Außerdem wurden keine Sensibilisierungskampagnen durchgeführt, und einige Mitarbeiter schienen nur ein begrenztes Verständnis für Cyberrisiken zu haben.

IDENTIFIZIEREN

Auf der Grundlage der bereitgestellten Informationen wurden die folgenden Details über den Vorfall gesammelt:

- ☑ Es wurde eine sozial konstruierte Phishing-E-Mail mit einer komprimierten gezippten Datei empfangen, die als Nachweis für eine Lieferantenbestellung angehängt war.
- ☑ Beim Öffnen der Datei wurde die Malware auf dem Computer installiert
- ☑ Eine Keylogger-Software wurde installiert, die unbemerkt die Tastenanschläge des Computers überwacht und die Informationen an einen Cyberkriminellen sendet.
- ☑ Der Cyberkriminelle verwendet dann die erbeuteten Zugangsdaten, um auf das Bankkonto zuzugreifen und die Überweisung unter Verwendung gültiger Kontonummern und Passwörter vorzunehmen.
- ☑ Der Vorfall wurde erst erkannt, als der Cyberkriminelle versuchte, eine Überweisung von mehr als 1000 Euro vorzunehmen.

Antworten

Da das Unternehmen nicht über einen Cybersicherheitsplan verfügte, wurde die Reaktion auf den Angriff verzögert.

WER: Der Angreifer konnte nicht genau identifiziert werden. Nur eine E-Mail-Adresse war bekannt und die mögliche Herkunft.
WEM: nicht spezifisch
WARUM: Sammeln von sensiblen Daten und deren Verwendung zum Stehlen von Geld
WAS: Zugangsdaten für das Bankkonto des Unternehmens
WIE: Keylogger, überwacht unauffällig die Tastenanschläge des Computers

STRATEGIE: Die Bedrohung begann auf einem Computer ohne Antivirenprogramm. Der IKT-Experte eines Unternehmens führte einen Reinigungsprozess durch. Das Bankkonto wurde geschlossen und die Anmeldedaten geändert. Das IKT-Unternehmen half dem Unternehmen, eine vollständige Überprüfung der Cybersicherheit seiner Systeme durchzuführen und die Ursache des Vorfalls zu ermitteln. Außerdem empfahl das Unternehmen eine Aufrüstung der Sicherheitssoftware.

WIEDERHERSTELLEN

IMPACT: Das Unternehmen sperrte sein Bankkonto und leitete rechtliche Schritte ein, um seine Verluste zurückzuerhalten. Das Unternehmen erhielt einen kleinen Teil der Verluste zurück. Geld für Zeit und Anwaltskosten wurde nicht zurückerstattet.

WIEDERHERSTELLEN: Die Wiederherstellungsstrategie konzentrierte sich auf die Schließung des Bankkontos, um weitere Verluste zu vermeiden. Weitere Maßnahmen waren die Säuberung des angegriffenen Computers und des angegriffenen elektronischen Postfachs. Überprüfung aller Computer des Unternehmens auf weitere Angriffe.

STRATEGY: Das Unternehmen sollte verschiedene Maßnahmen ergreifen, um solche Vorfälle zu verhindern. Seine Strategie muss sich auf die folgenden Maßnahmen/Schritte konzentrieren:

- ☑ Umsetzung von Sicherheitsrichtlinien wie z. B. der Richtlinie zum Ändern von Passwörtern und der Richtlinie zur Verwaltung von Benutzerkonten.
- ☑ Installation und Pflege einer aktuellen Antivirus-/Antimalware-Software.
- ☑ Schulungsprogramme durchführen, um das Bewusstsein der Mitarbeiter zu schärfen.
- ☑ Schränken Sie webbasierte Inhalte ein.

- ☑ Regelmäßige Kontrollen und Audits durchführen.
- ☑ Prävention und Implementierung eines Risikomanagementsystems

LESSONS LEARNT

- ☑ Benachrichtigungen - richten Sie Transaktionswarnungen für alle Kredit- und Debitkarten und Bankkonten ein.
- ☑ Zugangskontrolle. Beschränken Sie den Zugang zu sensiblen Konten auf die Mitarbeiter, die ihn benötigen; ändern Sie Passwörter häufig.
- ☑ Das Unternehmen sollte sein Risiko einschätzen und die Möglichkeiten einer Cyber-Haftpflichtversicherung prüfen.
- ☑ Wählen Sie Banken, die mehrere Authentifizierungsebenen für den Zugriff auf Konten und Transaktionen anbieten.
- ☑ Erstellen, pflegen und üben Sie einen Reaktionsplan für Cybervorfälle, der schnell umsetzbar ist.
- ☑ Cyberkriminelle verbreiten und installieren bösartige Software per E-Mail. Schulen Sie Ihre Mitarbeiter in Sachen E-Mail-Sicherheit.

FALLSTUDIE 17: EIN GESTOHLENER COMPUTER VERURSACHT EINE SCHWERWIEGENDE DATENVERLETZUNG

BETROFFENE ORGANISATION

Ein 10-köpfiges Beratungsunternehmen schickte ein kleines Team nach Ungarn, um ein Kundenprojekt abzuschließen. Während des Aufenthalts ließ der leitende Berater sein Arbeitslaptop, das Zugang zu sensiblen Kundeninformationen und Bankdaten des Unternehmens hatte, in einem verschlossenen Auto zurück, während er einen Auftrag ausführte. Das Auto wurde aufgebrochen, und der Laptop wurde gestohlen. Leider waren die Daten auf dem PC unverschlüsselt, da der Mitarbeiter die Unternehmensrichtlinie zur Verschlüsselung aller sensiblen Daten auf seinem PC nicht befolgt hatte. Das Unternehmen befürchtete nun einen Cyberangriff auf seine Systeme, Bankkonten und den Verlust von Kundendaten.

Art des Angriffs: Physischer Diebstahl eines unverschlüsselten PCs. Bei der Verschlüsselung wird lesbarer Text verschlüsselt, so dass er nur von der Person gelesen werden kann, die den Entschlüsselungscode besitzt. Damit wird eine zusätzliche Sicherheitsebene für sensible Informationen geschaffen.

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die zur Beschreibung des Vorfalls benötigten Informationen wurden durch ein Interview mit dem leitenden Berater des Unternehmens und dem IT-Techniker des IKT-Unternehmens, das die Beratungsfirma unterstützt, gesammelt. Die Interaktion wurde unter der Bedingung durchgeführt, dass sensible Informationen anonym bleiben. Auch wenn der Befragte bereit war, den Vorfall zu beschreiben, konnten einige verschlüsselte Informationen nicht erlangt werden, weshalb das unterstützende IKT-Unternehmen gebeten wurde, den Fall aufzuklären.

VORBEUGEN

Obwohl es sich bei dem Vorfall nicht um einen eindeutigen Cyberangriff handelt, handelt es sich um einen schwerwiegenden und sehr häufigen Vorfall, der eine Reihe von bedeutenden Cyberangriffen verursacht.

Im Fall des untersuchten Unternehmens gab es im Hinblick auf die Cybersicherheit spezifische Strategien und Mechanismen, die jedoch von einigen Mitarbeitern aufgrund ihrer geringen Erfahrung im Bereich der Informations- und Cybersicherheitsrisiken nicht umgesetzt wurden.

IDENTIFIZIEREN

Der Angestellte meldete den Diebstahl sofort bei der Polizei und seiner Firma. Auch die Bank wurde informiert, um die Kontobewegungen zu überwachen. Das Unternehmen informierte daraufhin die IKT-Firma, die den Fernzugriff des Laptops deaktivierte, und begann mit der Überwachung der Aktivitäten. Der Laptop war mit Sicherheitstools und einem Passwortschutz ausgestattet. Die auf der Festplatte gespeicherten Daten waren nicht verschlüsselt - darunter auch sensible Kundendaten und Bankdaten des Unternehmens.

Für eine verhaltensbasierte Identifizierung dieses Angriffs können die folgenden MITRE ATT&CK-Techniken verwendet werden:

- ☑ T1027 - Verdeckte Dateien oder Informationen
- ☑ T1036 - Maskerade
- ☑ T1586.002 - Kompromittierte Konten: E-Mail-Konten

ANTWORTEN

Antwort: Das Unternehmen muss die staatlichen Gesetze in Bezug auf eine Datenschutzverletzung befolgen. Die staatlichen Gesetze und die EU-Verordnungen über GPDR sind sehr streng und sehen hohe Geldstrafen vor.

- ☑ **WER:** Der Angreifer konnte nicht identifiziert werden. Nur der Ort des Vorfalls war bekannt.
- ☑ **WEM:** nicht spezifisch
- ☑ **WARUM:** Sammeln sensibler Daten und Erzielen von Gewinnen aus dem Verkauf der gestohlenen Geräte
- ☑ **WAS:** Sensible Daten von Kunden und die Bankdaten des Unternehmens
- ☑ **WIE:** Verlust von Ausrüstung, Verlust sensibler Daten und Angriff auf Bankkonten
- ☑ **STRATEGIE:** Die Bedrohung begann auf einem Computer ohne Antivirenprogramm und hat sich seitlich ausgebreitet. Eine Reinigung wurde von einem spezialisierten IT&C-Unternehmen durchgeführt.

WIEDERHERSTELLEN

IMPACT: Das Beratungsunternehmen gab mehr als 20.000 Euro für die Umsetzung, Überwachung und operative Verbesserungen aus. Eine Datenschutzverletzung wirkt sich negativ auf eine Marke aus, und das Vertrauen muss wiederhergestellt werden.

Die wichtigsten Folgen des Angriffs waren folgende:

- ☑ Daten Verlust
- ☑ PC Verlust
- ☑ System Kompromisse

☑ Finanzielle Kosten

WIEDERHERSTELLEN: Die Wiederherstellungsstrategie konzentrierte sich auf die Minimierung der Markenreputation und die Überwachung und Kontrolle der internen Systeme und Bankkonten des Unternehmens. Vorbeugend wurden alle Zugangsdaten für Bankkonten geändert und die Systemprivilegien der Mitarbeiter ausgesetzt und geändert.

STRATEGIE: Das Unternehmen sollte verschiedene Maßnahmen ergreifen, um solche Vorfälle zu verhindern. Seine Strategie muss sich konzentrieren auf

- ☑ Durchführung von Schulungsprogrammen, um das Bewusstsein der Mitarbeiter zu schärfen
- ☑ Durchführung von regelmäßigen Kontrollen und Audits
- ☑ Durchführung Prävention und Implementierung eines Risikomanagementsystems

LESSONS LEARNT

- ☑ Die Unternehmen müssen die Mitarbeiter im sicheren Umgang mit den am Arbeitsplatz bereitgestellten Geräten schulen.
- ☑ Die Geräte müssen sicher aufbewahrt werden, wenn sie sich nicht in unmittelbarer Nähe des Mitarbeiters befinden.
- ☑ Die Unternehmen müssen Maßnahmen ergreifen, um Daten zu verschlüsseln, wo immer sie gespeichert oder übertragen werden.
- ☑ Die Mitarbeiter sollten sich über die Bedeutung der Verschlüsselung und deren Anwendung im Klaren sein.
- ☑ Die Unternehmen müssen ihre Verantwortlichkeiten im Rahmen der Gesetze zur Meldung von Datenschutzverletzungen des Landes, in dem sie tätig sind, kennen und verstehen.
- ☑ Eine regelmäßige Überprüfung der Sicherheitspraktiken des Unternehmens ist in modernen Organisationen unerlässlich, um Vorfälle zu verhindern, Schwachstellen zu entdecken und die Auswirkungen von Vorfällen zu verringern

FALLSTUDIE 18: DDOS-ANGRIFF STOPPT WICHTIGE DIENSTE

BETROFFENE ORGANISATION

Bei der angegriffenen Organisation handelte es sich um einen Hosting-Anbieter. Die Angreifer führten Mitte Dezember 2021 einen massiven Distributed-Denial-of-Service-Angriff gegen eine bestimmte Website durch, der eine Bandbreite von 1,5 Gigabit pro Sekunde und fast 100 Millionen Pakete pro Sekunde überschritt - der größte Angriff, dem ein Hosting-Unternehmen ausgesetzt war.

Das Unternehmen geht davon aus, dass sich der Angreifer auf Websites mit Online-Casino-Spielen konzentrierte und der Hosting-Anbieter nicht das eigentliche Ziel war. Der DDOS-Angriff führte dazu, dass die Verfügbarkeit der Dienste des Kunden für mehr als 12 Stunden unterbrochen wurde.

Ein DDoS-Angriff (Distributed Denial of Service) ist ein böswilliger Versuch, den normalen Datenverkehr eines Servers, eines Dienstes oder eines Netzes zu stören, indem das Ziel oder die umliegende Infrastruktur mit einer Flut von Internetdaten überschwemmt wird. DDoS-Angriffe erreichen ihre Wirksamkeit, indem sie mehrere kompromittierte Computersysteme als Quellen für den Angriffsverkehr nutzen. Zu den angegriffenen Maschinen können Computer und andere vernetzte Ressourcen wie IoT-Geräte gehören.

"Im Jahr 2019 wurden 57 % mehr Mirai-Botnet-Varianten identifiziert. Mirai-Varianten werden in der Regel für Brute-Force-Angriffe auf IoT-Geräte verwendet. Diese Angriffe nahmen um 51 % zu, während Web-Exploits im Jahr 2019 um 87 % zunahmen." (MCCART, 2022).

WIE DIE INFORMATIONEN ERWORBEN WURDEN?

Die Informationen, die zur Beschreibung dieses Cyberangriffs benötigt wurden, wurden durch zwei Interviews (persönliche Treffen) gesammelt, eines mit dem Geschäftsführer des Unternehmens und eines mit einem IT-Techniker des Unternehmens. Beide waren bereit, den Vorfall zu beschreiben und Einzelheiten zu nennen, baten aber darum, die beiden Unternehmen und ihre Namen anonym zu halten, da die Informationen für sie zu sensibel waren.

VORBEUGEN

Obwohl der Hosting-Anbieter über mehrere Cybersicherheitsverfahren und -mechanismen verfügt, haben die Angreifer offenbar eine Schwachstelle gefunden, die sie ausnutzen konnten.

Die Techniker des Unternehmens bemerkten, dass die Website plötzlich langsam wurde, aber sie gehen davon aus, dass es sich um einen legitimen Anstieg des Datenverkehrs aufgrund der Urlaubszeit handelte. Der Angriff wurde kurz nachdem die Website nicht mehr erreichbar war und der Kunde sich beschwerte, festgestellt.

IDENTIFIZIEREN

Die Angreifer nutzten Datenverkehr aus weltweiten Quellen. Es scheint, dass der Denial-of-Service-Angriff von einem Mirai-Botnetz erstellt wurde. Und da das Mirai-

Botnetz in der Lage ist, rund 600 Megabit pro Sekunde zu senden, verwendeten sie einen Angriff der zweiten Ebene mit einem anderen Mirai-Botnetz.

Mirai ist eine Malware, die intelligente Geräte mit ARC-Prozessoren infiziert und sie in ein Netzwerk von ferngesteuerten Bots oder "Zombies" verwandelt. Dieses Netzwerk von Bots, ein so genanntes Botnet, wird häufig für DDoS-Angriffe verwendet.

Der Hosting-Anbieter nutzte Tools zur Analyse des Datenverkehrs, um den Angriff zu erkennen. Das Hauptmerkmal des Angriffs ist das hohe Aufkommen, das von ein und derselben Reihe von IP-Adressen ausgeht. Den Technikern gelang es, diese IPs zu isolieren, und die Website war wieder erreichbar.

Danach versuchten sie herauszufinden, warum das Verkehrsanalysetool den Angriff nicht von Anfang an erkannt hatte.

Nach dem MITRE ATT&CK-Rahmenwerk kann dieser Vorfall wie folgt beschrieben werden:

- ☑ T1499 - Denial of Service für Endgeräte
- ☑ T1498 - Netzwerk Denial of Service

ANTWORTEN

- ☑ **WER:** Der Angreifer kann nicht identifiziert werden. Der Angriff kam aus der ganzen Welt
- ☑ **WEM:** Das Ziel war eine bestimmte Website, auf der Online-Casinospiele angeboten wurden.
- ☑ **WARUM:** Zur Unterbrechung des Betriebs.
- ☑ **WAS:** Website des Unternehmens.
- ☑ **WIE:** DDOS-Angriff über Mirai-Botnets.
- ☑ **STRATEGIE:** Der Angriff begann bei einem Server eines Hosting-Anbieters, um den Betrieb einer bestimmten Website zu unterbrechen. Das Tool zur Analyse des Datenverkehrs hat es versäumt, auf die Möglichkeit eines Cyberangriffs hinzuweisen. Das Unternehmen hat die Empfindlichkeit der Alarme im Verkehrsanalysetool erhöht, um ähnliche Vorfälle in Zukunft zu vermeiden.

WIEDERHERSTELLEN

IMPACT: Der Hosting-Anbieter hatte erhebliche Zusatzkosten, um den Angriff abzuwehren, und auch sein Ruf war ernsthaft geschädigt. Hinzu kamen die zusätzlichen Arbeitskosten für die Wiederherstellung der Website und die Vertragsstrafen im Rahmen der SLA-Vereinbarung mit dem Kunden. Die Gesamtkosten wurden auf etwa 40 000 € geschätzt.

WIEDERHERSTELLEN: Die Wiederherstellungsstrategie konzentrierte sich darauf, die angreifenden IPs zu isolieren, um den Angriff zu stoppen und den Betrieb der Website wiederherzustellen. Weitere Maßnahmen bestanden darin, die Alarmempfindlichkeit des Verkehrsanalysetools zu erhöhen. Überprüfung aller Hosting-Server und -Dienste auf weitere Angriffe oder verdächtige Aktivitäten.

STRATEGIE: Das Unternehmen sollte verschiedene Maßnahmen ergreifen, um solche Vorfälle zu verhindern. Seine Strategie muss sich konzentrieren auf

- ☑ Erhöhen Sie die Empfindlichkeit des Verkehrsanalysetools
- ☑ Installieren Sie ein zweites Tool für zusätzliche Sicherheit
- ☑ Schulungsprogramme durchführen, um das Bewusstsein der Mitarbeiter zu schärfen
- ☑ Beschränken Sie einige IP-Bereiche
- ☑ Regelmäßige Kontrollen und Audits durchführen
- ☑ Durchführung Prävention und Implementierung eines Risikomanagementsystems
- ☑ Ihre Infrastruktur und Dienste nach ISO27001 und ISO22301 zertifizieren.

LESSONS LEARNT

- ☑ Unterbrechungen gibt es in vielen Formen. Unterbrechungen oder Verzögerungen können viele Formen annehmen, insbesondere für Hosting-Anbieter. Wenn ein Angriff festgestellt wird, müssen die entsprechenden Reaktionsteams Ressourcen bereitstellen, um ihn zu bewältigen.
- ☑ Viele Cyberangriffe sind leicht zu verhindern. Ausgeklügelte Cyberangriffe können großen Schaden anrichten, aber viele von ihnen lassen sich mit den richtigen Sicherheitsmaßnahmen leicht verhindern. Es ist wichtig, ein starkes und proaktives Sicherheitsmanagementsystem aufzubauen, um die Angriffe zu stoppen. Ein solches Managementsystem erfordert eine kontinuierliche Wartung, die Überwachung aller Systeme und Geräte im Netz, einschließlich der Aktualisierung der Technik und der Anwendung von Sicherheits-Patches für bekannte Schwachstellen.
- ☑ DDoS-Angriffe sollten ernst genommen werden. Die heutigen DoS- und DDoS-Angriffe sind anders, da sie bösartiger, gezielter und leistungsfähiger sind.
- ☑ Kein Zeitlimit. Angriffe auf der Netzwerkebene können länger als 48 Stunden dauern, während Angriffe auf der Anwendungsebene tagelang andauern können. Die Infiltration von Systemen und Netzwerken zum Zwecke des Ausspionierens kann Wochen und Monate dauern.
- ☑ Cybersicherheit sollte eine Priorität sein. Cybersicherheit sollte für alle Unternehmen, die in der heutigen Landschaft tätig sind, eine der höchsten Prioritäten sein. Diese Angriffe sind inzwischen ausgeklügelt, zielgerichtet, leistungsfähig und unreguliert. Alle Bedrohungen sollten ernst genommen werden, auch DDoS-Angriffe, die immer häufiger vorkommen.

ZUSAMMENFASSUNG

Auf der Grundlage des breit gefächerten Portfolios, das in der ENCRYPT 4.0-Dokumentenbatterie zu Cyberangriffen vorgestellt wird, können die folgenden Schlussfolgerungen gezogen werden:

- ☑ **Mit der Entwicklung der IKT und im Kontext von Industrie 4.0** gewinnt die Cybersicherheit immer mehr an Bedeutung, und Unternehmen, die sich nicht angemessen gegen Cyberangriffe schützen, setzen ihre Geschäftstätigkeit einem ernsthaften Risiko aus.
- ☑ **Die Mitarbeiter spielen eine Schlüsselrolle bei der Cyberverteidigung**, daher sollten Mitarbeiter sowohl in KMU als auch in großen Unternehmen zumindest eine Grundausbildung zum Schutz von Unternehmensdaten und zur Arbeit mit sensiblen Informationen erhalten, da mehr als viele Cyberangriffe auf mangelndes Wissen über diese Aspekte zurückzuführen sind, insbesondere im Zusammenhang mit der Fernarbeit während der COVID-19-Pandemie.
- ☑ KMU werden unabhängig von der Branche, in der sie tätig sind, zu primären Zielen für Hacker und organisierte Cyberkriminelle, aber gleichzeitig hat nur ein Drittel der KMU einen Plan, wie ein potenzieller Cyberangriff abgewehrt werden kann; daher müssen KMU der Cybersicherheit oberste Priorität einräumen, um ihre Wettbewerbsfähigkeit langfristig zu sichern.

REFERENZEN

1. Acronis, 2020. The NHS cyber-attack. [Online] Acronis. Erhältlich bei :https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/

2. Barber, B., 2016. William Hill apologise after website attack. [Online] Racing Post. Erhältlich bei: https://www.racingpost.com/news/william-hill-apologise-after-website-attack/266196 (Case study 6)

3. Blue goose, n.d. Information Security at William Hill. [Online] blue goose. Erhältlich bei: https://bluegooseis.co.uk/work/william-hill (Fallstudie 6)

4. Braue, D., 2022. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. [Online] 2022 Cybersecurity Ventures. Erhältlich bei: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

5. Cook, S., 2022. 20+ DDoS attack statistics and facts for 2018-2022. [Online]. Comparitech. Erhältlich bei: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

6. Craver, R., 2015. Hanesbrands database hacked 900K phone, online customers affected. [e-journal] *Winston-Salem Journal.* Erhältlich bei: https://journalnow.com/business/hanesbrands-database-hacked/article_543b338e-3664-11e5-b77e-c77df1e08b5c.html (Fallstudie 4)

7. Cyber Startup Observatory. Erhältlich bei: https://cyberstartupobservatory.com/ (Fallstudie 4)

8. CyberNews, 2021. Thousands of Humana customers have their medical data leaked online by threat actors. [Online] 2022 Cybernews. Erhältlich bei: https://cybernews.com/news/humana-insurance-customers-medical-data-leaked/ (Case study 5)

9. CyberTalks, 2022. Top 15 phishing attack statistics (and they might scare you) [Online]. CyberTalks. Erhältlich bei: https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

10. Cyware , 2018. Humana websites hit by sophisticated spoofing attack from 'foreign countries'. [Online] Cyware. Erhältlich bei: https://cyware.com/news/humana-websites-hit-by-sophisticated-spoofing-attack-from-foreign-countries-5ac77624 (Fallstudie 5)

11. Dissent, 2018. Humana notifies members after credential stuffing attack on Humana.com and Go365.com. [online] 2009 – 2022, DataBreaches.net and DataBreaches LLC. Erhältlich bei: https://www.databreaches.net/humana-notifies-members-after-credential-stuffing-attack-on-humana-com-and-go365-com/ (Fallstudie 5)

12. EUROPOL, n.d. World's most dangerous malware EMOTET disrupted through global action. [Online] EUROPOL 2022. Erhältlich bei: https://www.europol.europa.eu/media-

press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

13. Kolbasuk McGee, M., 2018. Humana Notifying Victims of 'Identity Spoofing' Attack. [online] *Data Breach Today*. Erhältlich bei: https://www.databreachtoday.asia/humana-notifying-victims-identity-spoofing-attack-a-11153 (Fallstudie 5)

14. McCart, C., 2022. 15+ Shocking botnet statistics. [Online] Comparitech. Erhältlich bei:https://www.comparitech.com/blog/information-security/botnet-statistics/

15. Mimecast, 2022. Confronting the NEW WAVE OF CYBER ATTACKS: The State of Email security Report 2022. Mimecast. Erhältlich bei: https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-2022.pdf

16. Moore, J., 2022. Top 10 List of Cybersecurity Facts for 2022. [Online] Elevity. Erhältlich bei: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

17. Morran, Ch., 2015. Hanes Website Is The Latest, Oddest Victim Of Data Breach. Consumerist. Erhältlich bei: https://consumerist.com/2015/07/30/hanes-website-is-the-latest-oddest-victim-of-data-breach/ (Fallstudie 4)

18. StackHawk, 2022. What is Command Injection? [Online]. StackHawk, Erhältlich bei: https://www.stackhawk.com/blog/what-is-command-injection/

19. The Cyber Wire, n.d. Definition of Spoofing. [Online]. The Cyber Wire. Erhältlich bei: https://thecyberwire.com/glossary/spoofing

20. VentureBeat, 2022. Report: Average time to detect and contain a breach is 287 days. [Online] VentureBeat. Erhältlich bei: https://venturebeat.com/2022/05/25/report-average-time-to-detect-and-contain-a-breach-is-287-days/

21. Verizon, 2021. DBIR: 2021 Data Breach Investigation Report. Verizon, 2021. Erhältlich bei: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

22. Wallarm, 2021. The Biggest Hacker Attacks on Gambling. 10. [Online] Wallarm. Erhältlich bei: https://lab.wallarm.com/the-biggest-hacker-attacks-on-gambling/ (Fallstudie 6)

ENCRYPT 4.0

Co-funded by the Erasmus+ Programme of the European Union

PROJEKT PARTNER

ENCRYPT 4.0

Gemeinsame Initiative zur Entwicklung von Cyber-Fachkräften soll der europäischen Industrie helfen, den Mangel an Fachkräften im Bereich Cybersicherheit zu beheben

Das Projekt ENCRYPT4.0 (2020-1-RO01-KA202-079983) zielt darauf ab, das Management von KMU des verarbeitenden Gewerbes in die Lage zu versetzen, einen proaktiven Ansatz in Bezug auf die Cybersicherheit zu verfolgen, indem es sie bei der Analyse, Identifizierung und Bewältigung der Cyberrisiken und -bedrohungen unterstützt, die für ihr Unternehmen gelten. Durch die Förderung von interaktivem projektbasiertem Lernen im Hinblick auf die Verbesserung der Cybersicherheitsfähigkeiten und -kompetenzen von KMU-Mitarbeitern oder/und Cybersicherheitsexperten.

"George Emil Palade" Universität für Medizin, Pharmazie, Wissenschaften und Technologie ausTârgu Mureș - Rumänien

Projekt Koordinator

European Center for Quality Ltd., Beratunsgfirma - Bulgariien

Instituto de Soldadura e Qualidade, Technische Institution - Portugal

Avantalia, KMU Spainien

FH Joanneum, Fachhochschule - Österreich

PCX Management, IT GmbH. - Zypern