ENCRYPT 4.0

Inițiativa comună de dezvoltare a forței de muncă cibernetice pentru a permite industriei europene să depășească deficitul de profesioniști în securitate cibernetică

Nr. 2020-1-RO01-KA202-079983

O3: Baterie documentară despre atacuri cibernetice

Cofinanțat prin programul Erasmus+ al Uniunii Europene

CUPRINS

INTRODUCERE

Odată cu apariția Ti și dezvoltarea celei de-a patra revoluții industriale, companiile se confruntă cu noi provocări legate de securitatea cibernetică și protecția datelor. Acest lucru este valabil mai ales pentru IMM-urile de producție care adesea nu au resursele interne și capacitatea de a evalua în mod eficient riscurile de securitate cibernetică corespunzătoare tehnologiilor nou implementate bazate pe Industria 4.0. În același timp, IMM-urile devin mai des victimele diferitelor infracțiuni cibernetice. Potrivit celui mai recent Raport Verizon 2021 privind investigațiile privind încălcarea datelor *(Verizon, 2021)*, IMM-urile sunt victimele și sunt mult mai vulnerabile la atacuri cibernetice în comparație cu marile întreprinderi, deoarece le lipsesc resurse, oameni, informații și capacitatea generală de a evita riscurile unei atac cibernetic.

Între timp, amenințările cibernetice au surse diferite și devin din ce în ce mai sofisticate, de exemplu, și dacă echipele nu s-au confruntat cu vulnerabilități similare și nu au o îndrumare clară cu privire la modul de a răspunde la acestea, poate dura zile și chiar săptămâni pentru a reacționa corect, ceea ce poate fi fatal pentru unele procese de fabricație. Potrivit Raportului de securitate TI din 2021 al IMM-urilor, angajații care nu respectă liniile directoare sunt considerați ca fiind principala barieră în calea securității cibernetice, iar această tendință s-a înrăutățit odată cu dezvoltarea muncii la distanță din cauza pandemiei COVID-19 *(Untangle, 2021)*. Cu toate acestea, atunci când există o încălcare a securității cibernetice, aceasta nu afectează numai oamenii, ci poate provoca pierderi financiare, pierderea încrederii clienților și deteriorarea reputației *(Acronis, 2021).*

Ținând cont de cele menționate mai sus, consorțiul Encrypt 4.0 a dezvoltat acest document pentru a servi ca un instrument de know-how care oferă acces la analiza critică a atacurilor cibernetice reale și a lecțiilor învățate, precum și la foi de parcurs cu privire la modul de prevenire, identificare, abordare și recuperarea acestora.

Bateria documentară Encrypt 4.0 privind atacurile cibernetice este adaptată în mod special nevoilor IMM-urilor producătoare din UE care operează în contextul Industriei 4.0 și reprezintă o compilație de studii de caz privind atacurile cibernetice, care vizează sprijinirea IMM-urilor în creșterea securității lor cibernetice și prevenirea atacurilor cibernetice.

STRUCTURĂ ȘI METODOLOGIE

Bateria documentară Encrypt 4.0 conține un total de **18 studii de caz**. Fiecare dintre partenerii ENCRYPT 4.0 a dezvoltat 3 studii de caz reale privind atacurile cibernetice, bazate pe cercetări de birou, experiența personală și observații și interviuri amănunțite cu directori generali, profesioniști în securitate cibernetică și specialiști IT care acoperă diferite tipuri de atacuri cibernetice și oferă analize critice a motivelor încălcărilor de securitate, a modului în care au fost abordate și care au fost consecințele.

Consorțiul ENCRYPT 4.0 a construit un model specific „PREVENȚIE-IDENTIFICARE-RĂSPUNS-RECUPERARE” (PIRR) bazat pe modelul „Identificare, Protecție, Detectare, Răspuns și Recuperare” al Institutului Național de Standarde și Tehnologie (NIST). Tipul atacurilor cibernetice se bazează pe modelul STRIDE, precum și pe cadrul MITRE ATT&CK. Analiza modelului PIRR conține 4 categorii/secțiuni principale bazate pe pașii majori pentru combaterea unei probleme de securitate cibernetică, precum și secțiunile învățate (vezi Fig. 1).

Fig.1. Categoriile modelului „Prevenire – Identificare – Răspuns – Recuperare” (PIRR).

PREVENIRE

Această secțiune se concentrează pe reducerea riscului de expunere la atacuri cibernetice și măsuri preventive pentru fiecare studiu de caz care cuprinde următoarele:

- Practici specifice de securitate care au fost instituite și au avut efecte dovedite în atacurile cibernetice reale;
- Concepții greșite de securitate cibernetică: practici pe care fiecare companie le-a aplicat și au avut impact zero sau chiar negativ în incidentele reale.

IDENTIFICARE

Scopul principal al acestei secțiuni este de a ajuta IMM-urile să facă distincția între diferitele tipuri de atacuri cibernetice clasificate folosind modelul STRIDE și cadrele MITRE ATT&CK. Modelul STRIDE reprezintă un model de amenințare la nivel înalt centrat pe sistem, axat pe identificarea categoriilor generale de atacuri. Are următoarele 6 categorii:

+Falsificarea

+Alterarea

+Repudierea

+Dezvăluirea informației

+Refuzarea serviciului

+Ridicarea privilegiilor

În scopul studiilor de caz ENCRYPT 4.0, STRIDE a fost folosit pentru a identifica amenințările la nivel superior, în timp ce cadrul MITRE ATT&CK a fost aplicat pentru a pewzenta atacurile mai detaliat. Cadrul ATT&CK ia în mod intenționat punctul de vedere al atacatorului pentru a ajuta organizațiile să înțeleagă modul în care adversarii abordează, se pregătesc și execută cu succes atacurile.

RĂSPUNS

Această secțiune descrie situațiile în care amenințarea este deja prezentă, oferind o analiză a atacurilor cibernetice reale și sfaturi despre cum să reacționați în cazuri similare după identificarea acestora.

Atacurile cibernetice din studiile de caz sunt prezentate în următorul format:

- CINE: atacatorul
- CINE: organizația țintă
- DE CE: motivele din spatele atacului (a fost aleatoriu sau vizat)
- CE: proprietatea vizată
- CUM: descrierea atacului și care au fost tehnicile folosite.
- STRATEGIE: cum a fost abordată amenințarea și măsurile care au avut efect zero sau negativ.

RECUPERARE

Secțiunea oferă informații despre care au fost consecințele atacului, precum și analize cu privire la modul de a efectua o recuperare a sistemului după ce unele procese au fost deteriorate și de a recâștiga accesul la datele care s-au pierdut, pe baza cazurilor reale de atac descrise în secțiunea RĂSPUNS. Secțiunea urmează modelele STRIDE & MITRE ATT&CK care descriu practicile de recuperare bazate pe fiecare grup specificat de amenințări cibernetice prezentate în secțiunea IDENTIFICARE.

STUDII DE CAZ

STUDIU DE CAZ 1: COCHILA INVERSĂ

ORGANIZAȚIA ȚINTĂ

Asociația Innovalia este un centru tehnologic privat și independent care a fost creat de Grupul Innovalia cu scopul de a reuni o masă critică capabilă să își atingă cu succes ambițiile de cercetare pe termen lung și obiectivele strategice. Innovalia este o alianță pentru IMM-uri cu profil tehnologic, care are sediul central în Spania. Are o prezență internațională cu birouri în Țara Bascilor, Madrid, Catalonia, Insulele Canare, Europa, Asia, Orientul Mijlociu și America Centrală și de Sud. Încă de la înființare, Asociația Innovalia a dezvoltat o sensibilitate și conștientizare deosebită față de caracteristicile particulare ale IMM-urilor cu profil tehnologic. Astăzi, a devenit lider în domeniul cercetării și dezvoltării de către și pentru IMM-urile din Spania. De asemenea, oferă soluții pentru facilitarea proceselor internaționale de inovare destinate IMM-urilor. În calitate de agent tehnologic al Rețelei Tehnologice din Țara Bascilor (Innobasque), Innovalia reunește competențele, laboratoarele și resursele companiilor care au fondat asociația.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile pentru acest studiu de caz au fost adunate printr-un interviu aprofundat cu tehnicianul TI al întreprinderii. În timpul discuției, intervievatorul a pus întrebări astfel încât respondentul să fie încurajat să răspundă. Informațiile lipsă au fost completate a posteriori cu datele furnizate de persoana intervievată.

PREVENIRE

Practica pe care Innovalia a aplicat-o înainte de incident a fost instalarea unui **software firewall**.

Practici specifice de securitate:

- ☑ **conștientizarea angajaților cu privire la e-mailurile suspecte**. În acest caz, un hacker a trimis un e-mail aparent legitim în care le cere angajaților noștri să facă clic pe un link din e-mail pentru a reseta parola de acces, sub pretextul că au fost înregistrate mai multe încercări de conectare nereușite.
- ☑ **instalarea de firewall-uri interne** pentru a consolida firewall-ul extern standard. Când personalul lucra de acasă în timpul pandemiei de COVID-19, li s-a cerut să instaleze un firewall în rețeaua lor de acasă.

IDENTIFICARE

"Injecția de comandă este un atac cibernetic în care un atacator preia controlul asupra sistemului de operare gazdă prin injectarea de cod într-o aplicație vulnerabilă printr-o comandă. Acest cod este executat indiferent de orice mecanism de securitate și poate fi folosit pentru a fura date, a bloca sistemele, a deteriora bazele de date și chiar pentru a instala programe malware care pot fi utilizate ulterior". (StackHawn, 2022)

Tipul și natura atacului cibernetic a fost: **Injecții de cod într-o vulnerabilitate din serverul web apache al companiei prin executarea comenzilor de la distanță**. Acest tip de atac poate fi descris în detaliu conform cadrului MITRE ATT&CK, așa cum se arată mai jos.

- ☑ Recunoaștere: Scanare activă: Scanare blocuri IP și Scanare vulnerabilități.
- ☑ Acces inițial: Servicii externe la distanță.
- ☑ Execuție: Interpret de comandă și scripting: Powershell.
- ☑ Escaladarea privilegiilor:
  - Proces de injectare: Injecție de bibliotecă de legături dinamice; Injecție portabilă executabilă; Deturnarea executării firelor; Apel de procedură asincronă; Stocare locală de fire; Apeluri de sistem Ptrace; Memorie Proc; Injecție de memorie suplimentară pentru fereastră;
  - Execuție declanșată de eveniment: modificarea configurației Shell Unix.
- ☑ Evaziunea Apărării: Injecție de proces și șablon.
- ☑ Exfiltrare: Transferați date în contul Cloud.
- ☑ Impact:
  - Manipularea datelor: manipularea datelor stocate, transmise și în timpul executării;
  - Oprire serviciu;
  - Oprire/Repornire a sistemului.

RĂSPUNS

- ☑ **CINE:** Atacatorul nu a putut fi identificat cu precizie. Doar locul de origine, China, era cunoscut.
- ☑ **PE CINE:** Asociația Innovalia.
- ☑ **DE CE:** A fost întâmplător.
- ☑ **CE:** Sistemul organizației Innovalia.
- ☑ **CUM:** Injecția procesului cu executarea comenzii de la distanță.
- ☑ **STRATEGIE:** Amenințarea a fost atacată cu firewall-ul pe care îl are serverul în acel moment. Urmați pașii descriși în secțiunea următoare, despre cum să blocați IP-urile.

RECUPERARE

Principalele consecințe ale atacului au fost:

- ☑ Compromisul sistemului
- ☑ Cercetare și Analiză
- ☑ Actualizarea versiunii serverului
- ☑ Schimbați acreditările

Strategia de recuperare a fost axată pe blocarea IP-ului prin firewall:

În primul rând, conectați-vă la serverul pe care trebuie să blocați adresa IP. Apoi, faceți clic pe Start, tastați Windows Firewall cu securitate avansată și apăsați Enter. În panoul din stânga, faceți clic pe Reguli de intrare pentru a afișa regulile configurate curent în panoul din mijloc.

În panoul din dreapta, faceți clic pe Acțiuni > Regulă nouă: pentru Tip regulă, selectați Personalizat și faceți clic pe Următorul; pentru Program, selectați Toate programele și faceți clic pe Următorul; pentru Protocol și porturi, selectați Oricare din meniul drop-down Tip protocol și faceți clic pe Următorul; iar pentru Domeniu de aplicare: sub Ce adrese IP la distanță se aplică această regulă?, selectați opțiunea radială: Aceste adrese IP: Faceți clic pe Adăugare.

Apoi, introduceți adresa IP pe care doriți să o blocați de pe server și faceți clic pe OK. De asemenea, puteți alege să blocați o serie de adrese IP selectând opțiunea Acest interval de adrese IP: radial. După ce ați terminat de adăugat adresele IP, faceți clic pe Următorul. Pentru Acțiune, selectați Blocare conexiunea și faceți clic pe Următorul. Pentru Profil, lăsați toate opțiunile bifate și faceți clic pe Următorul. Pentru Nume, dați regulii un nume descriptiv, cum ar fi IP-uri pe lista neagră. De asemenea, puteți introduce o descriere opțională a regulii. Faceți clic pe Terminare. Regula nou creată cu numele dat se afișează acum în panoul din mijloc Reguli de intrare. Pentru a ordona regulile în ordine alfabetică după nume, puteți da clic pe antetul coloanei Nume. Dacă trebuie să dezactivați regula, faceți clic dreapta pe regulă din listă și faceți clic pe Dezactivați regula. Dacă trebuie să modificați domeniul de aplicare al adreselor IP pentru regulă, faceți clic dreapta pe regulă din listă și faceți clic pe Proprietăți. Apoi faceți clic pe fila Scop, faceți modificările necesare și faceți clic pe Aplicare.

LECȚII ÎNVĂȚATE

Am aflat că este mai bine să avem anumite măsuri preventive și defensive, care sunt utile pentru acest tip de atacuri, precum:

- ☑ Se menține serverul actualizat
- ☑ Se adăuga monitorizare la server
- ☑ Se segmentează rețeaua în VLAN-uri și
- ☑ Se izola aparatele care sunt expuse mediului exterior.

STUDIU DE CAZ 2: NEPĂSAREA UNUI ANGAJAT

PREVENIRE

Organizația a aplicat Sistemul de detectare a intruziunilor (IDS), care monitorizează rețeaua CARSA pentru activități rău intenționate sau încălcări ale politicii. CARSA aplică software firewall pentru a-și proteja rețeaua și sistemul împotriva accesului neautorizat.

Practicile specifice de securitate instituite care au avut efecte dovedite în alte atacuri cibernetice sunt:

Validați și igienizați intrările: Scanați caractere de escape și alte simboluri speciale pentru limba aplicației și sistemul de operare, cum ar fi marcajele de comentariu, caracterele de terminare a liniei și delimitatorii de comandă. Dacă aplicația se așteaptă doar la un set limitat de valori, acceptați numai acele valori, de exemplu prin includerea pe lista albă sau pornirea lor condiționată.

Evitați constructele de evaluare vulnerabile: evitați să folosiți „eval()” și funcții echivalente pe intrările brute ale utilizatorului. CARSA a folosit funcții dedicate specifice limbii pentru a procesa în siguranță argumentele furnizate de utilizator.

Închideți interpretul: Dacă aveți control asupra configurației serverului, este mai bine să limitați funcționalitatea interpretului la minimul necesar aplicației pentru a preveni escaladarea la injectarea comenzii de sistem. De exemplu, dacă aplicația dvs. PHP nu folosește funcția system(), puteți dezactiva acea funcție în fișierul dvs. php.ini specificând-o în directiva disable_functions: exec(), passthru(), shell_exec(), system(), proc_open(), popen(), curl_exec(), curl_multi_exec(), parse_ini_file() și show_source().

Verificați codul nostru: CARSA a folosit instrumente de verificare statică a codului pentru a scana vulnerabilități legate de validarea intrărilor și evaluarea nesigură.

Scanați aplicațiile: organizația a folosit un scaner pentru a se asigura că aplicațiile sunt protejate de diferite tipuri de atacuri. De exemplu, CARSA are un sistem de detectare a intruziunilor.

„În 2021, 83% dintre organizații au raportat că au suferit atacuri de phishing. În 2022, se așteaptă să aibă loc încă șase miliarde de atacuri.” (CyberTalk, 2022)

IDENTIFICARE

Atacul cibernetic a avut loc în cadrul CARSA și tipul de atac cibernetic a fost **‘atac phishing**’. Atacul de phishing este un tip de atac de inginerie socială folosit adesea pentru a fura datele utilizatorilor, inclusiv acreditările de conectare.

Conform modelului STRIDE, acest tip de atac are drept „Amenințare” înălțarea privilegiului, deoarece proprietatea încălcată este „autorizarea”. În acest tip de atac cibernetic, utilizatorul permite cuiva să facă ceva ce nu este autorizat să facă.

Conform cadrului MITRE ATT&CK, acest atac este:

☑ Recunoaștere: phishing pentru informații: serviciu de spearphishing, atașament de spearphishing și link de spearphishing.

☑ Acces inițial: Phishing: Atașamente de spearphishing, link sau prin serviciu.

☑ Execuție: Adversarii pot trimite mesaje de phishing pentru a obține acces la sistemele victimei. Toate formele de phishing sunt furnizate electronic prin ingineria socială. Phishingul poate fi vizat, cunoscut sub numele de spearphishing. În spearphishing, o anumită persoană, companie sau industrie va fi vizată de adversar. În general, adversarii pot desfășura phishing nedirecționat, cum ar fi campaniile de spam în masă cu programe malware.

☑ Descoperire: detectarea se poate face prin: Jurnalul aplicației (conținut), fișierul (crearea fișierului) sau traficul de rețea (conținut sau flux).

☑ Mișcare laterală: spearphishing intern.

☑ Exfiltrare: Inginerie socială și atacuri de phishing; e-mail de ieșire, descărcări pe dispozitive nesigure, încărcări către servicii externe și comportament nesigur în cloud.

☑ Impact: pierderea datelor sensibile, deteriorarea reputației, pierderea clienților sau a consumatorilor, costul perioadei de nefuncționare etc.

RĂSPUNS

CINE: Atacatorul era o persoană/organizație externă necunoscută, prin intermediul unui angajat CARSA.
PE CINE: Acreditările pentru accesul la un software de plată (fără public sau open-source).
DE CE: Furtul de acreditări, precum și de informații sensibile ale entităților.
CE: Date și parole.
CUM: Un angajat a instalat software care nu a fost permis de companie, așa cum este definit în politica companiei. Acest tip de software nu a fost permis din cauza fiabilității și securității dubioase (În general, toate programele care sunt instalate pe computerele angajaților trebuie să fie supravegheate de personalul tehnic informatic al entității). Acest software avea un cal „Trojan" de rețea. Există mai multe moduri în care un troian atacă un sistem, iar în acest caz particular, a fost un „troian infostealer", care așa cum sună, acest troian urmărește date de pe computerul vostru infectat.
STRATEGIA: Strategia aplicată a fost de a urmări adresa mac pentru a identifica mașina infectată și angajatul responsabil. Ulterior, software-ul a fost eliminat, precum și virusul.

RECUPERARE

IMPACT: furtul acreditărilor de utilizator la nivel local.

STRATEGIA DE RECUPERARE:

☑ Prin adresa MAC știam ce angajat este atacat, fără ca acesta să-și dea seama.
☑ A fost dezinstalat un software care nu ar fi trebuit instalat.
☑ Pe mașina respectivă au fost executate programe antivirus și antimalware.
☑ Acreditările de utilizator compromise au fost schimbate.

O STRATEGIE MAI BUNĂ: întregul computer ar fi putut fi formatat deoarece nu poți fi niciodată sigur de eliminarea lui completă.

LECȚII ÎNVĂȚATE

Creșterea responsabilității angajaților prin:

- ☑ Instruire cu prelegeri scurte despre importanța neinstalării de software neanunțat și confirmare de securitate din partea echipei de suport tehnic și,
- ☑ Rememorarea politicilor de securitate ale companiei și a reglementărilor comune de siguranță în domeniul securității cibernetice.
- ☑ Să actualizeze software-ul mașinilor companiei (software: Windows și programe antivirus). Să le reamintească angajaților să ruleze scanarea antivirus de mai multe ori.

STUDIU DE CAZ 3: CARDUL DE CREDIT ÎNTR-UN IMM prin rețeaua WIFI

THE ORGANIZAȚIA ȚINTĂ

Bodegas Monje este situată într-o enclavă excepțională a insulei Tenerife, în locul cunoscut sub numele de „La Hollera" din municipiul El Sauzal, cu vedere la Teide. O tradiție îndelungată a producătorilor de vin însoțește familia Monje încă din 1750. Butoaiele de stejar și sistemele moderne de macerare coexistă pentru a conferi vinurilor roșii, albe și roze un caracter și arome deosebite, care sunt perfect adaptate celei mai bune gastronomi a Insulelor Canare. Această cramă găzduiește, de asemenea, inițiative culturale, gastronomice și de agrement care extind granițele vinului și îl readuc în mediul social din care provine istoric, un adevărat angajament pentru turismul vinicol: Wine &Tours.

CUM S-A OBȚINUT INFORMAȚIA?

Metoda aplicată pentru colectarea informațiilor pentru acest STUDIU DE CAZ a fost un interviu în profunzime.

PREVENIRE

Organizația nu a aplicat nicio practică de securitate cibernetică înainte de acest eveniment. Au doar un firewall în furnizorul de servicii de internet (Router Movistar).

Practicile specifice de securitate instituite în Bodegas Monje care au avut efecte dovedite în prevenirea acestui gen de evenimente au fost

programate după eveniment. În special, acțiunile întreprinse au avut succes în prevenirea altor atacuri de natură similară.

IDENTIFICARE

Un client al unității a accesat compania pentru a consuma produsele fabricate și s-a conectat la internet prin intermediul rețelei WIFI. Atacul cibernetic a fost identificat chiar de clientul afectat. Această persoană a detectat operațiuni în conturile sale bancare cu plăți online efectuate cu cardul său de credit, dar nu de către el. Toate aceste operațiuni au fost făcute imediat după ce a vizitat compania „Bodegas Monje".
Clientul a alertat banca să încerce să anuleze acele plăți și să blocheze cardul pentru a împiedica infractorul cibernetic să-l folosească în continuare.
Ulterior, a anunțat compania „Bodegas Monje" deoarece acesta a fost ultimul loc în care a folosit CARDUL.

RĂSPUNS

CINE: client al unei companii care a accesat rețeaua locală în scopuri ilegale.
PE CINE: unui alt client, prin intermediul companiei.
DE CE: pentru furtul de bani.
CE: deturnarea de detalii bancare și aplicarea de taxe, beneficiind de banii altcuiva.
CUM: infiltrarea prin rețeaua Wifinet a clienților.
STRATEGIA: Reproiectarea rețelei prin separarea conexiunii clienților care vizitează afacerea de sistemul de plată și rețeaua internă a companiei.

RECUPERARE

IMPACT:

- ☑ Cardul de credit al unui client al unității este compromis.
- ☑ Încrederea clienților în securitatea companiei ar putea fi compromisă și nu s-ar putea baza pe efectuarea plăților prin această metodă atât de ușoară.
- ☑ Dacă mai mulți clienți ar fi afectați de acest atac cibernetic, acesta ar avea un impact direct asupra reputației companiei.

STRATEGIA DE RECUPERARE:

Strategia dusă de proprietarul companiei, din momentul în care a luat cunoştinţă de incident, a fost oprirea wifi-ului şi/sau deconectarea reţelei de oaspeţi. Apoi, a contactat o companie de securitate cibernetică pentru a o rezolva.

Noua strategie de recuperare realizată de echipa de securitate cibernetică a fost reproiectarea rețelei pentru a separa rețeaua clienților de rețeaua

internă a companiei unde sunt stocate cele mai sensibile date (datele proprii ale angajaților și clienților, cum ar fi datele sistemului de plată).

Nu au putut fi recuperați bani furați după ce rețeaua a fost reproiectată. Clientul a trebuit să schimbe vechiul card de credit „furat" cu altul nou. Persoana care a efectuat atacul cibernetic nu a putut fi identificată. Nu s-au putut lua măsuri legale.

Există o strategie mai bună de întreprins în această situație. În loc să deconectați rețeaua wifi a companiei, următoarele acțiuni ar fi putut fi făcute suplimentar:

- ☑ Să întocmească o listă cu toate informațiile compromise, cu toate datele de contact ale posibililor clienți care ar putea fi afectați (după cronologie – a celor care se aflau în întreprindere în același timp cu clientul afectat).
- ☑ Să informeze alți clienți să fie conștienți de orice mișcări ciudate în conturile lor bancare efectuate cu plăți online efectuate cu cardul lor de credit.
- ☑ Să colecteze cât mai multe informații posibil, nu numai pentru a putea identifica vinovatul atacului cibernetic, ci și pentru a avertiza mai bine clienții care ar putea fi afectați.
- ☑ Schimbarea imediată a parolelor pentru a evita o închidere bruscă a companiei, deoarece în acel moment, rețeaua nu era divizată, funcționa atât pentru clienți, cât și pentru angajați.

LECȚII ÎNVĂȚATE

Dintre lecțiile învățate se remarcă următoarele:

- ☑ că este mai bine să avem rețeaua segmentată
- ☑ că trebuie implementate politici de zero-trust
- ☑ că nu trebuie să fii o companie mare pentru a suferi un atac cybernetic
- ☑ că este necesar să existe echipamente la zi și sisteme active de securitate cibernetică (cu firewall profesional, IPS, antivirus etc.).

STUDIU DE CAZ 4: DEZVOLTAREA INFORMAȚIILOR HANESBRANDS INC.

ORGANIZAȚIA ȚINTĂ

Hanesbrands Inc. (HBI) este o companie multinațională de îmbrăcăminte fondată în 1901 cu sediul în Winston-Salem, SUA. Au peste 250 de magazine în 47 de țări. Printre cele mai cunoscute mărci ale companiei se numără Hanes, Champion, Playtex, Bali, L'eggs, Just My Size, Barely There, Wonderbra, Duofold, Celebrity, Maidenform, Zorba etc. Unul dintre avantajele competitive ale Hanesbrands este că 70% din articolele de îmbrăcăminte pe care le vând sunt fabricate în propriile sedii, precum și în cele ale partenerului contractual. În acest fel, compania reușește să controleze majoritatea lanțului de aprovizionare, ceea ce permite, de asemenea, stabilirea unor practici puternice de sustenabilitate și contribuie la succesul său la nivel mondial. În 2021, HBI a fost desemnată de Ethisphere una dintre cele mai etice companii din lume și a devenit parte a „Cele mai sustenabile 100 de companii Barron" trei ani la rând. Pentru a se asigura că compania urmează o politică de durabilitate pe termen lung, a stabilit obiective globale de sustenabilitate pentru 2030 (în conformitate cu Obiectivele de dezvoltare durabilă ale Națiunilor Unite sub trei piloni: oameni, planetă și produs) și a lansat un site web de sustenabilitate.

În 2019, compania a avut venituri de 7,0 miliarde USD și aproximativ 61 000 de angajați. Se raportează că HBI cheltuiește peste 100 000 USD pentru securitatea cibernetică, folosind în principal produse Akamai, cum ar fi serviciile cloud.

CUM S-A OBȚINUT INFORMAȚIA?

Metoda aplicată pentru colectarea informațiilor pentru acest studiu de caz a fost cercetarea de birou, iar sursele de informații specifice pot fi găsite în secțiunea Referințe a acestui document.

PREVENIRE

☑ **Practici care au avut efect zero:** Autentificare pe site - Pentru a-și urmări comanda de îmbrăcăminte, utilizatorul a primit un link pentru a se autentifica ca invitat pe site. Utilizatorul invitat avea drepturi extinse de a obține informații pentru comenzile făcute de toți ceilalți utilizatori, doar prin modificarea adresei URL a invitatului. Prin urmare, baza de date a fost compromisă prin intermediul site-ului, deoarece nu a cerut autentificarea și a considerat utilizatorul invitat ca un utilizator valid. Datele vizibile pentru alți clienți constau în nume, ultimele cifre ale cărților de credit, adresa, numărul de telefon etc.

"Potrivit unui nou raport al Blumira și IBM, ciclul mediu de viață a încălcării durează 287 de zile, organizațiile având nevoie de 212 zile pentru a detecta inițial o încălcare și de 75 de zile pentru a o reține." (VentureBeat, 2022)

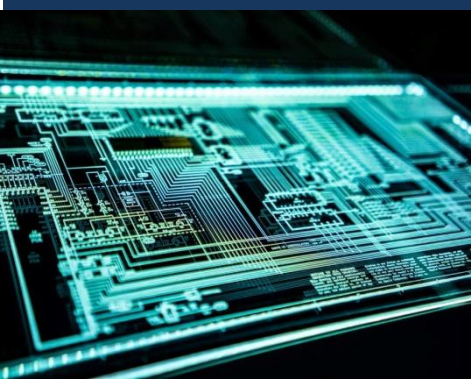
☑ **Practici care au avut efecte dovedite în atacurile cibernetice reale de acest tip:**

1. Descoperirea expunerii datelor (folosind sisteme de scanare externe).
2. Autentificarea puternică (Autentificarea unică care permite unui utilizator să se conecteze în mai multe sisteme diferite sau nume de utilizator/parole diferite pentru fiecare sistem).
3. Prioritizarea accesului la date (de exemplu, RU poate avea nevoie doar de acces la informațiile angajaților, iar departamentul de contabilitate poate avea nevoie doar de acces la datele bugetare și fiscale. În principiu, utilizatorii invitați ar trebui să aibă acces minim la date).
4. Implementarea infrastructurilor de monitorizare și a soluțiilor automate care pot identifica rapid problemele potențiale înainte ca acestea să devină urgențe, să izoleze bazele de date infectate și să semnaleze echipelor de asistență și TI următorii pași.

IDENTIFICARE

Atacul împotriva Hanesbrands Inc. a fost de **tipul de divulgare a informațiilor**.

În ultima săptămână din iunie și prima iulie 2015, Hanesbrands Inc. a fost victima unui atac cibernetic. După furtul datelor, compania a fost informată de adversari cu privire la încălcare fără a oferi un motiv pentru acțiunea lor. Este foarte probabil ca vulnerabilitatea companiei să fi fost descoperită prin scanare [1]. Hackerii au creat o comandă de check-out „oaspeți" pe site-ul Hanesbrands [2] (fără să se înregistreze măcar pe site). Odată cu linkul de



comandă primit, hackerii au reușit să descarce baza de date a companiei, care era responsabilă cu păstrarea datelor pentru toate comenzile clienților (comenzile care au fost făcute pe site-ul web sau prin telefon) – după cum s-a dovedit că prin linkul de check-out „oaspeți" s-a putut lansa orice comandă fără autentificare. Într-o săptămână, adversarii au reușit să obțină informații pentru peste 900 000 de clienți. Pentru a nu fi detectați, hackerii au folosit cel mai probabil Port Knocking [3] pentru a-și ascunde activitatea. Conform Hanesbrands, adversarii au folosit Capturi de ecran [4] pentru a extrage datele. Totuși este foarte probabil că au folosit un mod mai automat – cum ar fi un script care analizează direct datele [5].

Atacul descris de cadrul MITRE ATT&CK:
[1] Scanare activă: Scanarea vulnerabilități (T1592.002).
[2] Acces inițial: exploatează aplicația destinată publicului (T1190).
[3] Persistență: Semnalizarea traficului: Închiderea porturilor (T1205.001).
[4] Captură de ecran (T1113).
[5] Colectare automată (T1119).

Atacul a fost identificat de companie după ce a fost sesizat de adversari. Hanesbrands nu era conștient că acest lucru se întâmpla până când hackerii nu i-au anunțat.

RĂSPUNS

În iunie 2015, Hanesbrands Inc. a fost informată de adversari cu privire la încălcare. Prin contul de invitat de pe site-ul lor, atacatorii au reușit să extragă informații generale despre utilizatori pentru 900.000 de clienți. După ce a fost anunțat despre scurgere, Hanesbrands a adăugat autentificare la baza lor de date „comenzile clienților" și a eliminat opțiunea de „check-out pentru oaspeți" (chiar dacă au remediat-o).

CINE: Necunoscut.

PE CINE: Hanesbrands Inc.

DE CE: A fost un atac direcționat pentru a obține informații despre baza de date și listele clienților, dar adversarii nu au cerut nicio răscumpărare până la urmă. Tocmai au informat Hanesbrands că au obținut datele.

CE: Informații generale despre clienți pentru 900.000 de clienți – nume, adrese, informații despre starea comenzii clienților, numere de telefon și ultimele 4 cifre ale cardului lor de credit. Dar numele de utilizator sau parolele clienților nu au fost dezvăluite. Hackerii nu au compromis sistemele corporative ale Hanesbrands.

CUM: Adversarii au creat o comandă prin verificarea contului de oaspete pe site-ul Hanesbrands. Prezentându-se drept „oaspeți" care verifică o comandă (adversarii nu erau înregistrați pe site), au reușit să găsească o breșă în baza de date Hanesbrands exploatând link-ul comenzii. Hackerii au putut accesa detaliile și starea comenzilor clienților și au putut extrage

datele timp de aproximativ o săptămână folosind opțiunea „exploat with check-out” de pe site.

STRATEGIA: Odată ce Hanesbrands a fost notificat despre încălcare de către adversari, ei au adăugat autentificare la baza lor de date pentru a opri sursa de divulgare a informațiilor. În plus, au reparat check-out-ul „utilizator invitat” prin care a fost gestionată scurgerea. Hanesbrands și-a notificat clienții despre încălcare prin e-mail și poștă. De la acel accident, Hanesbrands investește din ce în ce mai mult în securitatea cibernetică în fiecare an.

RECUPERARE

☑ **IMPACT:** Consecințele au fost scurgeri de informații generale despre clienți. Nu este dezvăluit niciun proces sau alte daune directe.

☑ **STRATEGIA DE RECUPERARE:** Hanesbrands și-a informat clienții despre încălcare. S-a reparat linkul „utilizator invitat” [1] pentru a nu avea acces direct la baza de date și dezactivarea generală ca opțiune [2]. Serviciul este oferit clienților pentru a răspunde dacă utilizatorii au nelămuriri. În plus, au efectuat un audit de securitate [3] și scanare a vulnerabilităților [4] la sistemele lor existente și au investit în cursuri de securitate cibernetică [5].

Atenuările descrise de cadrul MITRE ATT&CK:

[1] Configurare software (M1054).
[2] Dezactivați sau eliminați funcția sau un program (M1042).
[3] Audit (M1047).
[4] Scanarea vulnerabilităților (M1016).
[5] Ghid pentru dezvoltatori de aplicații (M1013).

☑ **O STRATEGIE MAI BUNĂ:** După repararea linkului „utilizator invitat” prin care un client își putea revizui achiziția, Hanesbrands îl dezactivează ca opțiune. În schimb, ar fi putut adăuga o monitorizare pentru activități suspecte și/sau politici pentru revizuirea doar a anumitor cantități de achiziții.

LECȚII ÎNVĂȚATE

Atacurile de dezvăluire a informațiilor devin foarte rare, deoarece multe instrumente moderne oferă securitate cibernetică automată în ele și consiliază companiile cu privire la ceea ce ar putea fi o posibilă scurgere. Atacul asupra Hanesbrands arată că pista slabă de auditare a bazei de date și lipsa expertizei în securitate pot fi exploatate destul de ușor. În multe cazuri, bazele de date sunt încălcate din cauza nivelului insuficient de expertiză în domeniul securității cibernetice și a lipsei de pregătire/educare relevantă a angajaților non-tehnici care, ca urmare, pot încălca regulile de bază de securitate a bazei de date. De asemenea, personalului IT i-ar putea lipsi expertiza necesară pentru a aplica politicile de securitate, a conduce procese și acțiuni adecvate de raportare a incidentelor.

Un alt aspect este că baza de date din Hanesbrand era vulnerabilă din cauza configurării greșite – bazele de date devin de obicei total neprotejate din această cauză. Se uită adesea că, de obicei, adversarii sunt specialiști TI de înaltă profesie, care știu cu siguranță să exploateze astfel de vulnerabilități. Acest lucru poate fi contracarat prin dezactivarea conturilor implicite ale bazei de date, combinată cu personal TI instruit și experimentat.

Hanesbrands a avut noroc că s-au scurs doar informații generale, precum și că adversarii au informat compania după ce au extras toate datele pe care le-au putut. În plus, Hanesbrands și-a informat

imediat clienții cu privire la încălcare, ceea ce arată că compania dorește să fie aproape de clienții săi, iar problema este luată în serios.

STUDIU DE CAZ 5: SPOOFING HUMANA

ORGANIZAȚIA ȚINTĂ

Humana este o companie de asigurări de sănătate cu sediul în Louisville, Kentucky. Înființată inițial în 1961 ca operator de azil de bătrâni, activitatea principală a companiei a trecut la deținerea și administrarea de spitale, apoi în anii 1980 la planuri de asigurări de sănătate. În mai 2015, Forbes a estimat că compania are o valoare de 26,7 miliarde de dolari. În 2020, Humana a avut venituri de 77,155 miliarde USD și aproximativ 48 000 de angajați. Lunar, Humana cheltuiește peste 100.000 USD pe securitate cibernetică. Humana utilizează produse de securitate cibernetică precum „Akamai" (platformă de livrare în cloud) și „Prolexic (soluții de securitate pentru protejarea site-urilor web, a centrelor de date și a aplicațiilor IP de întreprindere împotriva atacurilor Distributed Denial of Service (DDoS)), „Proofpoint" (soluție) pentru a vă proteja oamenii și datele critice de amenințările avansate prin e-mail), programele „Alert Logic" (detecție și răspuns gestionate cu mănușă albă) și altele.

"Spoofing is an attack technique that relies on falsifying data on a network in a way that enables a malicious site or communication to masquerade as a trusted one." (The Cyberwire Glossary, n.d.)

CUM S-A OBȚINUT INFORMAȚIA?

Metoda aplicată pentru colectarea informațiilor pentru acest studiu de caz a fost cercetarea de birou, iar sursele de informații specifice pot fi găsite în secțiunea Referințe a acestui document.

PREVENIRE

☑ **Practici care au avut efect zero:** Alerte pentru încercări eșuate de conectare – Humana a aplicat această practică înainte de incident. Nu a fost eficient, deoarece organizației i-a luat aproximativ o zi să ia măsuri ca răspuns la numeroasele încercări de conectare eșuate primite.

☑ **Practici care au avut efecte dovedite în atacurile cibernetice reale:**

1. Blocarea contului după încercarea eșuată de conectare.
2. Blocarea traficului pe internet din țări străine cu care organizația nu face afaceri.
3. Forțarea resetarii parolei.

IDENTIFICARE

Atacul împotriva Humanei a fost de tip **Spoofing.**

Pe 3 iunie 2018, Humana a fost ținta unui atac sofisticat de falsificare cibernetică care a avut loc pe Humana.com. În aceeași zi, Humana a luat

cunoștință de o creștere semnificativă a încercărilor de eroare de conectare de la adresele IP ale țărilor străine [1]. Pentru a nu dezvălui locația lor reală, adversarii au folosit Multi-Hop Proxies [2]. Volumul încercărilor de conectare la Humana.com a sugerat că a fost lansat un atac amplu și amplu. Natura atacului și comportamentele observate au indicat că atacatorul avea o bază de date mare de identități de utilizator și parole corespunzătoare care au fost introduse cu intenția de a identifica care ar putea fi valide pe Humana.com prin „forță brută" [3]. Numărul excesiv de erori de conectare sugerează că informațiile de autentificare nu provin de la Humana [4] (și cel mai probabil au fost cumpărate de pe web-ul „întunecat"). Pe 4 iunie, Humana a blocat IP-urile. Pe baza acestor fapte, acesta poate fi descris drept atac de falsificare a identității. Adversarii au colectat date [5] pentru aproximativ 65 000 de utilizatori, inclusive:

- ☑ Reclamații medicale, dentare și de vedere, inclusiv serviciile efectuate, numele furnizorului, datele serviciului, taxele și sumele plătite etc.
- ☑ Informații despre contul de cheltuieli, cum ar fi informații despre cheltuielile contului de economisire a sănătății și soldul.

După incident, Humana a luat măsuri suplimentare ca blocarea contului după încercarea eșuată de conectare, blocarea traficului de internet din țări străine cu care organizația nu face afaceri și forțarea resetării parolei.

Atacul descris de cadrul MITRE ATT&CK:
[1] Interpret de comandă și scripting: Network Device CLI (T1059.008).
[2] Proxy: proxy multi-hop (T1090.003).
[3] Forța brută: Umplerea cu acreditări (T1110.004).
[4] Adunarea de informații despre identitatea victimei: acreditări (T1589.001).
[5] Colectare automată (T1119).
Atacul a fost identificat prin alerte pentru erori de tentative multiple de conectare.

RĂSPUNS

- ☑ **CINE:** Necunoscut
- ☑ **PE CINE:** Humana
- ☑ **DE CE:** Furtul de identitate (probabil va fi vândut către terți)
- ☑ **CE:** Informații sensibile ale utilizatorilor (reclamații medicale, stomatologice și vizuale, inclusiv serviciile prestate, numele furnizorului, datele serviciului, taxele și sumele plătite etc.; informații despre contul de cheltuieli, cum ar fi informații despre cheltuielile contului de economisire a sănătății și soldul).
- ☑ **CUM:** Adversarii au colectat cantități mari de conturi și acreditări. Apoi, folosind proxy multi-hop, autentificarea forțată brută cu conturile pe care le aveau. După conectarea cu succes, adversarii au colectat date despre utilizatori prin transferuri de date de dimensiuni mici.

☑ **STRATEGIA:** Odată ce Humana a observat creșterea semnificativă a numărului de erori de încercare de autentificare, operatorii lor de securitate cibernetică au blocat adresele IP străine de la care au fost făcute încercările multiple de conectare. După aceea, Humana a forțat resetarea parolei pentru toate conturile despre care se știe că au fost încălcate și chiar a lansat un produs - oferind membrilor timp de un an o protecție împotriva furtului de identitate.

RECUPERARE

☑ **IMPACT:** Consecința a fost scurgerea de informații confidențiale ale utilizatorilor (reclamații medicale, stomatologice și vizuale, inclusiv serviciile prestate, numele furnizorului, datele serviciului, taxele și sumele plătite etc; informații despre contul de cheltuieli, cum ar fi informații despre cheltuielile contului de economisire a sănătății și soldul). După aceea au fost intentate multe procese pentru neglijență față de Humana. Nu există informații dacă procesele au fost câștigate de companie, prin care să se sugereze că rezultatele au fost probabil negative.

☑ **STRATEGIA DE RECUPERARE:** După ce a trecut o lună, Humana a notificat un număr de membri pentru a-i informa despre încălcarea datelor. De asemenea, a luat o serie de măsuri pentru a-și spori securitatea cibernetică, precum: 1) forțarea resetării parolei [1]; 2) implementarea de noi alerte pentru conectări reușite și eșuate [2] și 3) conturi blocate care au fost conectate la activități suspecte [3]. În plus, au implementat o serie de controale tehnice pentru a îmbunătăți securitatea portalului web (blocarea atacului de forță brută, apărarea prin injecție SQL [4], instalarea unui certificat de securitate anSSL [5] etc.). De asemenea, compania a blocat toate adresele IP străine care nu erau relevante pentru operațiunile sale [6].

Atenuările luate de Humana descrise de cadrul MITRE ATT&CK:

[1] Politicile parolei (M1027).
[2] Prevenirea intruziunilor în rețea (M1031).
[3] Politici de utilizare a contului (M1036).
[4] Configurare software (M1054).
[5] Inspecții SSL/TLS (M1020).
[6] Filtrarea traficul de rețea (M1037).

☑ **O STRATEGIE MAI BUNĂ:**

Humana ar fi putut notifica utilizatorii mai devreme. De asemenea, ar fi putut adăuga măsuri de securitate suplimentare, cum ar fi:

- Utilizarea autentificării bazate pe schimbul de chei între mașinile din rețeaua unei organizații sau autentificarea cu mai mulți factori pentru acces la distanță;
- Utilizarea unei liste de control al accesului pentru a refuza adresele IP private pe interfețele din aval;
- Implementarea filtrării atât a traficului de intrare cât și de ieșire;
- Configurarea routerelor și comutatoarelor - dacă este posibil - pentru a respinge pachetele care provin din afara rețelei locale a unei organizații care pretind că provin din interior;
- Activarea sesiunilor de criptare pe routerul unei organizații, astfel încât gazdele de încredere din afara rețelei sale să poată comunica în siguranță cu gazdele locale.

LECȚII ÎNVĂȚATE

Lecțiile învățate constau în necesitatea de a pune mai mult accent pe securizarea datelor personale ale utilizatorilor, organizarea de training-uri ale personalului pentru a crește gradul de conștientizare a amenințărilor cibernetice, pentru a notifica utilizatorii despre scurgeri de date din cauza numeroaselor procese de neglijență față de Humana după incident (Humana nu a dezvăluit nicio informație că un astfel de atac a avut loc, doar cu o lună mai târziu).

Efectele atacului nu au fost legate doar de cheltuielile pentru a face față atacului și proceselor, ci și de prejudiciul mare adus reputației Humana și fiabilității sale. Întrucât firma se află în sfera asigurărilor de sănătate, este esențial ca aceasta să aibă cele mai înalte măsuri de securitate și încredere a clienților săi, deoarece datele stocate în sistemele sale sunt foarte sensibile și confidențiale. De aceea, Humana a fost și rămâne o țintă de top pentru atacurile cibernetice cu mult înainte de cea specificată în acest caz și după aceea. Având în vedere acest lucru, eroarea de apreciere a gravității acestui atac ar putea fi considerată surprinzătoare.

STUDIU DE CAZ 6: REFUZAREA SERVICIULUI WILLIAM HILL

ORGANIZAȚIA ȚINTĂ

William Hill este o companie de jocuri de noroc online cu sediul în Londra, Anglia - fondată inițial în 1934 de William Hill. Compania și-a schimbat proprietarul de multe ori – fiind cumpărată pentru prima dată în 1971 de Sears Holdings. După ce a fost vândută de mai multe ori, în aprilie 2021 a fost achiziționată de Ceasars Entertainment. În 2020, compania a avut venituri de 1.324,3 milioane de lire sterline și 12.000 de angajați (8.000 în Marea Britanie) în 2021. Compania avea mai mult de 1.400 de magazine de pariuri, dar în 2019 a început să închidă peste 800 de magazine din cauza profiturilor scăzute, dar susținând că își va păstra personalul intact.
Lunar, William Hill cheltuiește peste 100.000 USD pentru securitatea cibernetică. Firma folosește produse de securitate cibernetică precum „Prolexic“ (soluții de securitate pentru protejarea site-urilor web, centrelor de date și aplicațiilor IP de întreprindere împotriva atacurilor Distributed Denial of Service (DDoS)), „Proofpoint” (soluție pentru protecția oamenilor și datelor critice) de amenințări avansate de e-mail), „F5 BIG-IP Application Security Manager” (paravan de protecție web flexibil pentru aplicații care securizează aplicațiile web în medii cloud tradiționale, virtuale și private), „Check Point” (își protejează clienții de atacurile cibernetice din a 5-a generație care au o rată de captare crescută în industria malware, ransomware și amenințări țintite avansate) etc.

CUM S-A OBȚINUT INFORMAȚIA?

Metoda aplicată pentru colectarea informațiilor pentru acest studiu de caz a fost cercetarea de birou, iar sursele de informații specifice pot fi găsite în secțiunea Referințe a acestui document.

PREVENIRE

☑ **Practici care au avut efect zero:**

1. Difuzarea rețelei Anycast – William Hill are un astfel de tip de apărare – care este utilă pentru a reține cantități uriașe de clienți care vizitează site-ul său web sau poate dizolva cantități uriașe de trafic de rețea nedorit (cum ar fi atacul DDoS). Această strategie funcționează de obicei pentru majoritatea cazurilor de atacuri DDoS.

2. Simpla creștere a lățimii de bandă a rețelei (cât trafic poate reține) nu sa dovedit a fi eficientă în acest atac.

☑ **Practici care au avut efecte dovedite în atacurile cibernetice reale de acest tip:**

1. Implementarea protecției DDoS la nivel de server – reguli suplimentare care ajută la identificarea și blocarea traficului de rețea rău intenționat.
2. Adăugarea difuzării rețelei Anycast terță parte – acest lucru poate ajuta companiile să își mărească enorm capacitatea de a prelua mult mai mult trafic de rețea sau de a gestiona atacurile DDoS.

IDENTIFICARE

Atacul împotriva lui William Hill a fost de **tip de refuzare a serviciului.**

La 1 noiembrie 2016, William Hill a fost ținta unui atac distribuit de înaltă performanță de tip denial of service [1]. Înainte de atac, adversarii au adunat informații despre detaliile rețelei site-ului lui William Hill [2]. După aceea, adversarii au aglomerat site-ul lui William Hill cu trafic, astfel încât acesta nu a putut funcționa corect. Atacul le-a interzis clienților să parieze la meciurile de marți seara din UEFA Champions League. Atacul asupra William Hill a fost realizat cu ajutorul unui malware numit „Mirai" [4], care creează o rețea de numeroase sisteme informatice cunoscute sub numele de „botnet" [3] pentru a începe atacul DDoS prin intermediul acestora.

Atacul descris de cadrul MITRE ATT&CK:
[1] Refuzarea serviciului în rețea: inundație direct în rețea (T1498.001).
[2] Adun[informații despre rețeaua victimelor: adrese IP (T1590.005).
[3] Achiziționare de infrastructură: botnet (T1583.005).
[4] Virus vierme cu autopropagare care utilizează baza de date cu acreditări implicite.
Cu aceste acreditări, dispozitivele IoT (dispozitive inteligente precum trackere de fitness, asistenți vocali, accesorii smarthome etc.) sunt scanate și infectate.
Atacul a fost identificat imediat după ce site-ul lui William Hill nu mai răspundea și nu mai era accesibil.

RĂSPUNS

CINE: Necunoscut.
PE CINE: William Hill.
DE CE: Încercări în afaceri – este foarte probabil ca rivalul companiei să facă astfel de acțiuni mai ales în timpul unor evenimente sportive populare precum UEFA Champions League / Extorsionare – dacă William Hill nu reușește să facă față situației este probabil să se solicite răscumpărare.
CE: Site-ul lui William Hill a fost oprit pentru o întrerupere de 24 de ore, ceea ce a cauzat pierderi de 4,4 milioane de lire sterline. Companiei William Hill i-au trebuit zile pentru a-și restabili complet site-ul și sistemele.

"According to Cloudflare, in Q4, 2021 the manufacturing industry received the most application-layer DDoS attacks, recording a 641% increase quarter-on-quarter in the number of attacks." (Cook, 2022)

CUM: Pe site-ul lui William Hill s-a desfășurat un atac de înaltă performanță Distributed Denial of Service cu rețeaua „botnet” (mai multe computere care au fost infectate cu virusuri malware și folosite pentru a efectua un astfel de atac fără știrea sau consimțământul lor) create de un malware numit „Mirai”.

STRATEGIA: După ce au observat că site-ul lor web este oprit, specialiștii IT de la William Hill au început să filtreze traficul de intrare. William Hill a folosit difuzarea rețelei Anycast – trimiterea traficului de rețea fiind difuzată peste rețeaua de servere ale companiei. Această atenuare distribuie traficul de rețea până la punctul în care traficul este absorbit de rețeaua companiei. Utilitatea acestei strategii depinde de cât de mare este rețeaua companiei și cât de mare este atacul DDoS. În cazul lui William Hill – chiar și cu infrastructura și securitatea sa de vârf nu au fost suficiente pentru a face față unui astfel de atac.

RECUPERARE

IMPACT: Atacul DDoS împotriva lui William Hill a făcut ca site-ul său să rămână închis timp de peste 24 de ore, în care clienții nu au putut paria pe meciurile UEFA Champions League. Acest lucru a dus la pierderi de peste 4,4 milioane de lire sterline într-o singură zi. Din fericire pentru William Hill, doar site-ul său a fost vizat, ceea ce a păstrat intacte datele sensibile ale utilizatorilor (care este un indiciu că adversarii au vrut să interzică utilizatorii să viziteze site-ul web și nu să fure date). A fost nevoie de peste 4 zile de lucru pentru ca specialiștii TI de la William Hill să-și revină site-ul web și sistemele afectate.

STRATEGIA DE RECUPERARE: Pentru a face față atacului, William Hill a filtrat traficul de rețea de intrare [1]. Filtrarea traficului de rețea – blocarea traficului numai pentru atac și permiterea unuia legitim. De asemenea, a început să folosească furnizori terți de difuzare a rețelei Anycast (companii care oferă un astfel de tip de serviciu - care dizolvă atacul DDoS atunci când împrăștie tot traficul de intrare prin rețeaua sa).

O STRATEGIE MAI BUNĂ:

☑ Gazda verifică starea de sănătate, care va alerta specialiștii IT ai companiei atunci când este detectată o utilizare anormală a rețelei [2]. Dacă sunt detectate la timp, pot fi întreprinse acțiuni pentru a menține disponibil serviciul site-ului.

☑ Se poate folosi „Rutarea găurilor negre”. Este o tehnică care direcționează atât traficul legitim, cât și cel rău intenționat, către o rută nulă și abandonată din rețea. Nu este o soluție ideală, deoarece face site-ul inaccesibil.

☑ Limitarea ratei. Limitează numărul de solicitări pe care serverul le poate primi - singur nu poate opri atacul DDoS, dar este un instrument util în strategia generală de apărare.

Strategia de recuperare descrisă de cadrul MITRE ATT&CK:

a. [1] Filtrați traficul de rețea (M1037).

b. [2] Sănătatea senzorului: starea gazdei (DS0013).

LECȚII ÎNVĂȚATE

Atacul împotriva lui William Hill ne poate arăta că chiar și o companie cu securitate cibernetică excepțională și una care este pregătită să facă față unor astfel de atacuri poate suferi din cauza lor.

Chiar dacă site-ul său a fost ferit de atacul DDoS (de obicei, astfel de atacuri sunt doar o cortină de fum pentru atacul propriu-zis), securitatea de nivel superior a companiei a fost intactă și funcțională, păstrând informațiile sensibile ale clienților în siguranță. Acest lucru le-a arătat clienților lor că sunt în siguranță și a păstrat credibilitatea companiei. Având în vedere că adversarii nu au mai încercat să exploateze vulnerabilitatea lui William Hill, arată că, cel mai probabil, atacul a fost făcut din cauza rivalității în afaceri (companie concurentă care dorește să profite de piața de pariuri) sau a unei tentative de extorcare (compania se bazează pe site-ul web, iar menținerea acestuia de către adversari generează pierderi).

Odată cu intrarea în era dispozitivelor inteligente (IoT) când totul poate fi operat de la distanță (lumini pentru casă inteligentă, aspiratoare, frigidere, ceasuri inteligente etc.), trebuie să ne gândim și la securitatea care trebuie aplicată. Toate aceste dispozitive inteligente au o adresă IP și pot fi sparte prin rețea – pentru obținerea de informații sau „zombificate” (dispozitivul vostru este controlat fără ca să știți și începe să funcționeze într-un mod ciudat) și folosit în atacuri DDoS pentru a inunda un site-ul web.

STUDIU DE CAZ 7: GRAVE DE COBALT: UTILIZAREA INSTRUMENTELOR ROȘII DE ECHIPARE DE CĂTRE CRIMINALI CIBERNICI

ORGANIZAȚIA ȚINTĂ

Cobalt Strike este un instrument de echipă roșie care a fost dezvoltat în 2012. Scopul său principal este de a ajuta echipele roșii să testeze și să simuleze atacurile cibernetice. Deoarece instrumentul are capabilități bune de a ocoli granițele de securitate prin evaziuni, atacatorii au deturnat unele versiuni ale acestuia pentru a-l abuza ca instrument de livrare pentru încărcături utile rău intenționate, cum ar fi ransomware. Acest studiu de caz nu se concentrează pe o singură organizație, deoarece Cobalt Strike este folosit pentru a efectua atacuri în masă care vizează diferite tipuri de organizații, cum ar fi fabrici, instituții financiare, companii de telecomunicații și multe altele.

CUM S-A OBȚINUT INFORMAȚIA?

Metoda aplicată pentru colectarea informațiilor pentru acest studiu de caz a fost cercetarea de birou, iar sursele de informații specifice pot fi găsite în secțiunea Referințe a acestui document.

PREVENIRE

Detectarea și prevenirea unui atac care utilizează instrumentul roșu de echipă Cobalt Strike implică un lanț de securitate în întreaga infrastructură. Acest lucru începe deja cu software-ul de protecție și monitorizare pe clientul terminal și merge până la nivelul rețelei. În plus, informațiile active privind amenințările sunt, de asemenea, necesare pentru a menține actualizate instrumentele de detectare bazate pe semnături.

Acest lucru implică de obicei:

- ☑ Securitate endpoint (cum ar fi antivirus, monitorizare bazată pe gazdă).
- ☑ Securitatea rețelei (cum ar fi firewall, proxy, detectarea semnăturii/modelului în trafic).
- ☑ Securitatea e-mailului.
- ☑ Politicile de gazdă/securitate configurate corect.

IDENTIFICARE

Cobalt Strike este un instrument comercial multifuncțional care îndeplinește diferite tehnici de atac. Având în vedere instrumentul și capacitățile sale în sine, acesta poate fi clasificat ca dezvăluire de informații și creștere a privilegiilor. Cu toate acestea, deoarece poate fi folosit și pentru a elimina încărcăturile utile rău intenționate, mai ales că au fost observate atacuri ransomware în combinație cu Cobalt Strike, lista poate fi extinsă cu Tampering și Denial of service.

Având în vedere toate caracteristicile instrumentului, acesta este un instrument de acces la distanță cu capacități de mișcare laterală. Acest lucru duce la o listă uriașă de tehnici de atac utilizate de Cobalt Strike și, prin urmare, vom acoperi doar câteva dintre ele aici.

- ☑ Mecanism de control al cotei abuzive (T1548).
- ☑ Odată ce Cobalt Strike a fost executat pe un sistem, acesta are capabilitățile de a efectua diverse tehnici utilizate pentru a obține permisiuni mai mari.
- ☑ Locuri de muncă BITS (T1197).
  BITS este un instrument Windows care poate fi folosit de Cobalt Strike pentru a descărca încărcături utile.
- ☑ Interpret de comandă și scripting (T1059).
  Cobalt Strike poate folosi diverse instrumente pentru a executa comenzi, coduri și scripturi. Aceasta include PowerShell, Windows Command Shell, Visual Basic, Python și JavaScript.
- ☑ Exploatarea pentru escaladarea privilegiilor (T1068).
- ☑ Pentru a obține privilegii mai mari, Cobalt Strike poate exploata vulnerabilitățile din sistemul de operare.

Captură de intrare (T1056)/Captură de ecran (T1113).
Cobalt Strike poate acționa și ca un keylogger și poate colecta capturi de ecran din sistemul infectat.

RĂSPUNS

- ☑ **CINE:** Necunoscut
- ☑ **PE CINE:** Mai multe organizații de pe tot globul.
- ☑ **DE CE:** Cobalt Strike a fost folosit în mai multe campanii concentrate pe diferite obiective. Motivul atacului este de a avea acces la rețeaua de organizare internă pentru deplasarea laterală. Un alt motiv ar putea fi acela de a provoca daune companiilor atacând rețeaua compromisă cu, de ex. un ransomware.
- ☑ **CE:** În principal pentru acces la distanță, compromis de rețea și mișcare laterală.
- ☑ **CUM:** Cobalt Strike este un instrument comercial roșu de echipă folosit pentru a simula atacurile cibernetice care au fost deturnate. Instrumentul este folosit pentru a obține accesul inițial la o rețea a companiei, precum și pentru acțiuni ulterioare cu rețeaua compromisă.
- ☑ **STRATEGIA:** În funcție de compania atacată, informațiile despre modul în care au identificat și au reacționat la atac sunt necunoscute.

RECUPERARE

- ☑ **IMPACT:** Atacatorul poate obține acces complet la rețea în cadrul companiei. Acest lucru poate duce la dezvăluirea de informații, precum și la alte atacuri care sunt livrate în funcție de operatorul atacului.
- ☑ **STRATEGIA DE RECUPERARE:** În funcție de compania atacată, informațiile despre cum arăta strategia lor de recuperare sunt necunoscute.
- ☑ **O STRATEGIE MAI BUNĂ:**
  - Păstrați sistemele antivirus la zi
  - Utilizați sisteme de detectare a intruziunilor și prevenirea lor
  - Monitorizați în mod corespunzător sistemele pentru activități suspecte
  - Configurați corect sistemele și dezactivați serviciile care nu sunt necesare
  - Conștientizarea angajaților
  - Utilizați segmentarea la nivel de rețea și limitați comunicarea permisă la minimum necesar

LECȚII ÎNVĂȚATE

Deși este necesar să se construiască instrumente roșii de echipă care să poată fi utilizate pentru simularea atacurilor într-o rețea pentru a găsi posibile puncte vulnerabile, trebuie totuși să rețineți că un astfel de instrument poate fi, de asemenea, compromis și utilizat de către un atacator.

STUDIU DE CAZ 8: ATAC ZIUA-ZERO – GRUPUL DE HACKERI HAFNIUM ȚINTESC SERVERE DE SCHIMB

ORGANIZAȚIA ȚINTĂ

Cercetătorii de la începutul anului 2021 au descoperit mai multe vulnerabilități critice în Microsoft Exchange Server, care au condus la exploatare masivă în întreaga lume. Vulnerabilitățile au fost folosite necontrolat de mai multe organizații criminale, în special de grupul HAFNIUM, înainte ca Microsoft să furnizeze patch-uri. Acest lucru a făcut ca atacurile să fie deosebit de greu de răspuns și de recuperat.

CUM S-A OBȚINUT INFORMAȚIA?

Metoda aplicată pentru colectarea informațiilor pentru acest studiu de caz a fost cercetarea de birou, iar sursele de informații specifice pot fi găsite în secțiunea Referințe a acestui document.

PREVENIRE

Zeci de mii de companii au fost afectate de acest atac. Din cauza expunerii generale a serverelor Microsoft Exchange la internet și a potențialului de ocolire a autentificării atacului, în primul rând a fost foarte greu de prevenit. Acest lucru conduce în continuare la ipoteza că diferitele practici de securitate care se aplică pentru acele companii au avut un impact zero.

IDENTIFICARE

Există patru vulnerabilități diferite care au condus la atacurile descrise. Vulnerabilitățile sunt **CVE-2021-26855, cunoscut ca ”ProxyLogon”, CVE-2021-27065, CVE-2021-26857 și CVE-2021-26858**. Tehnica de exploatare a acestor vulnerabilități este descrisă ca **“Exploatarea pentru Execuția Clientului” (T1203)** în cadrul MITRE ATT&CK.

CVE-2021-26855 este o ocolire de autentificare folosind proxy-ul intern de la Exchange Server. Cu aceasta, un atacator poate obține acces privilegiat direct la server. Combinând-o cu o altă vulnerabilitate precum CVE-2021-27065, care permite scrierea de fișiere arbitrare în sistem, sau CVE-2021-26857, pentru a obține acces la SISTEM (T1078) printr-o deserializare nesigură, acesta creează un lanț de exploatare fără restricții.

Atacurile au avut loc înainte ca Microsoft să poată lansa un patch pentru vulnerabilități. Potrivit numeroaselor resurse, acest interval de timp a fost de aproximativ 58 de zile de exploatare ziua-zero. Primul grup care a fost asociat cu aceste vulnerabilități a fost HAFNIUM. Mai târziu, mai multe alte grupuri au început să abuzeze de aceste vulnerabilități. Capacitățile atacului au permis scenarii multiple, de la exfiltrarea datelor (T1567) la implementarea de ransomware (T1486).

Mai jos este o listă a acțiunilor întreprinse de grupul HAFNIUM folosind acest vector de atac:

☑ T1589 – Colectarea adreselor de e-mail pentru utilizatorii pe care intenționau să-i vizeze

☑ T1071 – cadru C2 open source (de exemplu, acord)

☑ T1560 – 7-Zip, WinRAR pentru a comprima fișierele furate pentru extracție

☑ T1059 – Exportarea datelor cutiei poștale prin PowerShell

☑ T1567 – Exfiltrarea datelor prin site-uri de partajare, inclusiv MEGA

☑ T1105 – Descărcarea de programe malware și instrumente pe gazde compromise (de exemplu, Nishang, PowerCat)

☑ T1003 – Evacuarea acreditărilor pentru bazele de date LSASS și Active Directory (NTDS.DIT)

☑ T1505 – Implementarea WebShells pe gazde compromise (SIMPLESEESHARP, SPORTSBALL etc.)

Identificarea atacurilor poate avea loc datorită inspecției jurnalelor pe posibile mașini compromise. Microsoft a lansat îndrumări pentru detectarea fiecărei vulnerabilități în funcție de indicatorul lor de compromis.

RĂSPUNS

CINE: HAFNIUM (probabil UN grup sponsorizat de stat cu legături în China).
PE CINE: Diferite companii de pe tot globul, în principal industria americană.
DE CE: Exfiltrarea datelor și probabil câștigare de bani prin ransomware.
CE: Cunoștințe despre companie precum date, adrese de e-mail, cutii poștale.
CUM: Utilizarea mai multor vulnerabilități din Microsoft Exchange Server pentru a permite executarea de cod la distanță neautentificată.
STRATEGIA: Scanarea intervalului IP al internetului pentru a colecta liste de IP ale serverelor Microsoft Exchange. Exploatarea vulnerabilităților menționate pentru a implementa shell-uri web sau semnalizatoare C2. Utilizarea acestui acces a permis comprimarea și exfiltrarea datelor prin intermediul site-urilor web de partajare online precum MEGA. Ocazional, implementarea ransomware-ului „DearCry”. Acest lucru a fost posibil din cauza disponibilității târzii a patch-ului și a gestionării proaste a patch-urilor companiilor.

RECUPERARE

IMPACT: Consecințele acestui atac pot fi considerate pierderi de informații, deoarece atât exfiltrarea, cât și ransomware-ul se încadrează în această categorie. În plus, dacă organizațiile au încercat să plătească răscumpărarea pentru a-și recupera datele, au ajuns și la un prejudiciu financiar.

STRATEGIA DE RECUPERARE: În funcție de atacul specific, recuperarea poate diferi. Procesul de recuperare de la un ransomware poate dura mult

timp. Toate sistemele infectate trebuie fie reinstalate, fie o copie de rezervă trebuie să fie restabilită. Dacă copiile de rezervă au fost stocate pe un sistem infectat, evident că acestea nu pot fi folosite pentru procesul de recuperare. Recuperarea după exfiltrarea datelor este diferită. La început ar trebui aplicate patch-urile disponibile și urmele de învelișuri de rețea sau de semnalizatoare C2 trebuie îndepărtate. Este important să evaluăm care și câte date au fost furate pentru a măsura impactul.

O STRATEGIE MAI BUNĂ

- ☑ Păstrați sistemele antivirus la zi
- ☑ Folosiți sisteme de detectare a intruziunilor și prevenire a intruziunilor
- ☑ Monitorizați în mod corespunzător sistemele pentru activități suspecte
- ☑ Configurați corect sistemele și dezactivați serviciile care nu sunt necesare
- ☑ Gestionare rapidă a patch-urilor pentru a remedia vulnerabilitățile cât mai curând posibil
- ☑ Utilizați segmentarea la nivel de rețea și limitați comunicarea permisă la minimum necesar

LECȚII ÎNVĂȚATE

Exploatarea zero-day cu lanțuri de atac pare foarte intimidantă. Cheia pentru a face față acestor provocări este o segmentare adecvată a rețelei și monitorizarea sistemului pentru a identifica posibilele atacuri în timp util. Sistemele de prevenire și intruziune în rețea pot ajuta, de asemenea, la detectarea unor astfel de atacuri. Ceea ce este de asemenea important este că patch-urile pentru vulnerabilitățile critice trebuie aplicate cât mai curând posibil pentru a remedia în continuare vectorii de atac.
Ca o altă lecție învățată, se poate menționa că cercetătorii de securitate de la DevCore au detectat pentru prima dată vulnerabilitățile și au ajutat Microsoft în procesul de corecție. Acest lucru subliniază importanța cercetării independente de securitate.

CASE STUDY 9: WannaCry: CÂND UN RANSOMWARE PARALEZĂ SISTEMUL DE SĂNĂTATE

ORGANIZAȚIA ȚINTĂ

În 2017, un nou ransomware numit **WannaCry (WannaCrypt)** a vizat sistemul de operare Windows infectat mii și mii de clienți din întreaga lume. În loc să vizeze o anumită organizație, atacul a fost larg răspândit și a afectat o mulțime de companii din diferite domenii.

CUM S-A OBȚINUT INFORMAȚIA?

Metoda aplicată pentru colectarea informațiilor pentru acest studiu de caz a fost cercetarea de birou, iar sursele de informații specifice pot fi găsite în secțiunea Referințe a acestui document.

PREVENIRE

Mai multe companii au fost afectate de acest atac, ceea ce duce la presupunerea că diferitele practici de securitate care se aplică acestor companii au avut un impact zero.

IDENTIFICARE

WannaCry este o aplicație rău intenționată care este clasificată drept ransomware deoarece criptează fișierele specifice utilizatorului pe un sistem vizat. Acest lucru duce la falsificarea datelor și la distrugerea acestora, deoarece proprietarul sistemului infectat nu este capabil să decripteze fișierele. Ulterior, acest lucru se termină cu un atac de tip denial of service din cauza fișierelor și datelor lipsă.

Una dintre principalele caracteristici ale WannaCry este tehnica sa folosită pentru a căuta automat sisteme țintă potențiale pe care ransomware-ul încearcă apoi să le infecteze. Deoarece acest malware poate infecta alte sisteme de la unul deja infectat, este denumit și vierme. Pentru a atinge acest obiectiv, este utilizat un exploit pentru vulnerabilitatea software în protocolul SMB al Microsoft Windows numit Eternal Blue, care se mapează la MITRE ATT&CK ID T1210.

Înainte ca malware-ul să se răspândească și să infecteze alte sisteme, mai întâi trebuie să le caute și să le găsească. Acest lucru se realizează prin diferite tehnici, cum ar fi scanarea pentru sisteme la distanță (T1018), enumerarea sesiunii active desktop la distanță (T1563), scanarea pentru noi unități atașate pe sistemul infectat (T1120). Odată ce este găsit un potențial dispozitiv sau unitate la distanță, WannaCry încearcă să se copieze pe sistemul țintă și își execută comportamentul rău intenționat.

“Focarul WannaCry, a afectat peste 200.000 de computere din peste 150 de țări. Costă Regatul Unit 92 de milioane de lire sterline și generează costuri globale de până la 6 miliarde de lire sterline.” (Acronis, 2020)

Înainte ca ransomware-ul să-și înceapă criptarea, efectuează modificări pe sistemul infectat pentru a dezactiva opțiunile de recuperare, la care se referă T1490. După aceea, caută fișiere specifice utilizatorului în diferite directoare (T1083) și începe să cripteze fiecare fișier găsit (T1486). Pentru comunicarea cu serverul de comandă și control se utilizează rețeaua Tor (T1573/T1090).

Pentru o identificare bazată pe comportament a acestui atac, pot fi utilizate următoarele tehnici MITRE ATT&CK:

- ☑ T1210: Exploatarea serviciilor de la distanță
- ☑ T1018: Descoperirea sistemului de la distanță
- ☑ T1563: Deturnarea sesiunii de serviciu de la distanță (.002 RDP Hijacking)
- ☑ T1120: Descoperirea dispozitivelor periferice
- ☑ T1490: Inhibați recuperarea sistemului
- ☑ T1083: Descoperirea fișierelor și a directorului
- ☑ T1486: Date criptate pentru impact
- ☑ T1573: Canal criptat (.002 Criptografie asimetrică)
- ☑ T1090: Proxy (.003 Multi-hop Proxy)

RĂSPUNS

În 2017, un nou ransomware numit WannaCry (WannaCrypt) care vizează sistemul de operare Windows a infectat mii și mii de clienți din întreaga lume. În loc să vizeze o anumită organizație, atacul a fost larg răspândit. Companiile mari în care unii dintre ei își desfășoară afacerile în întreaga

lume, cum ar fi producătorul de mașini, au fost lovite de ransomware. Cu toate acestea, și alte grupuri organizaționale precum transportul public, serviciile de sănătate sau serviciile de telecomunicații au fost puternic afectate.

- ☑ **CINE:** Necunoscut
- ☑ **PE CINE:** Diferite companii de pe tot globul.
- ☑ **DE CE:** Atinge daune mari din cauza pierderii de date și probabil câștigi bani.
- ☑ **CE:** Cunoștințe despre companie, cum ar fi datele.
- ☑ **CUM:** Infectarea unui ransomware care a fost distribuit printr-o vulnerabilitate găsită în Microsoft Windows.
- ☑ **STRATEGIA:** Nota de răscumpărare folosită de WannaCry a apărut pe ecranul sistemelor care au fost infectate. Sistemele antivirus și firewall-urile au detectat infecția și răspândirea ransomware-ului și, prin urmare, nu au împiedicat sistemele pentru infecții și daune suplimentare.

RECUPERARE

IMPACT: Consecințele acestui atac pot fi considerate pierderi de informații, deoarece toate fișierele care au fost criptate de ransomware nu mai pot fi citite. În plus, dacă organizațiile au încercat să plătească răscumpărarea pentru a-și recupera datele, au ajuns și la un prejudiciu financiar.

STRATEGIA DE RECUPERARE: Procesul de recuperare de la un ransomware poate dura mult timp. Toate sistemele infectate trebuie fie reinstalate, fie o copie de rezervă trebuie să fie restabilită. Dacă copiile de rezervă au fost stocate pe un sistem infectat, evident că acestea nu pot fi folosite pentru procesul de recuperare.

O STRATEGIE MAI BUNĂ

- ☑ Păstrați sistemele antivirus la zi
- ☑ Folosiți sisteme de detectare a intruziunilor și prevenire a lor
- ☑ Monitorizați în mod corespunzător sistemele pentru activități suspecte
- ☑ Configurați corect sistemele și dezactivați serviciile care nu sunt necesare
- ☑ Gestionare rapidă a patch-urilor pentru a remedia vulnerabilitățile cât mai curând posibil
- ☑ Conștientizarea angajaților
- ☑ Utilizați segmentarea la nivel de rețea și limitați comunicarea permisă la minimum necesar

LECȚII ÎNVĂȚATE

Atacurile ransomware sunt obișnuite în zilele noastre și pot lovi toate companiile. Este foarte recomandat să urmați practicile de securitate cunoscute pentru a face infrastructura IT cât mai sigură posibil pentru a limita deteriorarea unui atac la minimum.

STUDIU DE CAZ 10: SPIONAREA DATELOR PRIVATE SENSIBILE

ORGANIZAȚIA ȚINTĂ

În toamna anului 2020, la nivel național a fost anunțată o nouă alertă de securitate. Acesta a precizat că multe entități publice și private au fost grav afectate, la fel ca și în alte valuri succesive anterioare, **de atacuri malware de tip EMOTET**, care au dus la numeroase probleme. EMOTET este un program malware care infectează computerele care rulează sistemul de operare Microsoft Windows prin link-uri sau atașamente rău intenționate infectate (de exemplu, PDF, DOC, ZIP etc.).

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile necesare pentru a descrie acest atac cibernetic au fost colectate printr-un interviu cu tehnicianul IT al companiei. Interacțiunea s-a realizat cu condiția păstrării în mod anonim a informațiilor sensibile. Chiar dacă intervievatul a fost dispus să descrie incidentul, unele informații nu au putut fi obținute deoarece problema a fost delegată unei firme specializate și a trebuit investigată separat.

PREVENIRE

Deși s-au desfășurat campanii de conștientizare de către entități și organizații specializate cu privire la măsurile ce trebuie luate, multe organizații publice și private au fost afectate, potrivit rapoartelor existente.

În cazul firmei analizate, din perspectiva securității cibernetice au funcționat proceduri și mecanisme specifice, dar acestea nu au fost suficiente din cauza experienței reduse în domeniul domeniului digital a unor lucrători.

IDENTIFICARE

Emotet este un troian asociat inițial cu frauda bancară care, din 2017, s-a limitat la spam și la distribuția secundară a sarcinilor utile. În prezent pot fi identificate numeroase variante de Emotet și, din păcate, acest malware continuă să evolueze în noi variante cu capabilități mai complexe și tehnici de evaziune.

Pe baza descrierilor furnizate și a suplimentării din rapoartele media, următoarele aspecte au fost implicate în incident:

- ☑ A fost primit un e-mail de phishing proiectat social, cu o arhivă zip atașată și cu parola inclusă în mesaj
- ☑ Programele malware au fost criptate și protejate cu parolă într-un fișier de arhivă
- ☑ Soluții anti-malware evitate prin utilizarea arhivelor protejate prin parolă ca atașamente
- ☑ Încărcătorul troian conținea cod benign dintr-un DLL Microsoft pentru a evita soluțiile antivirus
- ☑ Deturnarea firelor pentru a distribui coduri rău intenționate folosind arhive protejate cu parolă ca atașamente
- ☑ Sistemele compromise au fost utilizate pentru a trimite e-mailuri rău intenționate altor persoane de contact
- ☑ Sistemele de e-mail se închid temporar pentru a opri răspândirea în continuare a troianului

☑ Rețele interne afectate

Conform cadrului MITRE ATT&CK, această incidență poate fi descrisă după cum urmează:

1. T1566.001 – Atașament de spearphishing
2. T1204.002 - Execuție utilizator: fișier rău intenționat
3. T1027 - Fișiere sau informații acoperite
4. T1036 – Mascarada
5. T1586.002 – Conturi compromise: Conturi de e-mail
6. T1586.002 – Conturi compromise: Conturi de e-mail
7. T1499 - Refuzarea serviciului de la punctul final
8. T1498 - Refuzarea serviciului în rețea

"EMOTET a fost mult mai mult decât un simplu malware. Ceea ce a făcut EMOTET atât de periculos este că malware-ul a fost oferit spre închiriere altor infractori cibernetici pentru a instala alte tipuri de malware, cum ar fi troieni bancari sau ransomware, pe computerul unei victime.." (EUROPOL, 2022)

RĂSPUNS

CINE: Atacatorul nu a putut fi identificat cu precizie. Doar locul de origine, Vietnam, era cunoscut.
PE CINE: Fără țintă specifică
DE CE: Colectare de date sensibile și plăți pentru ransomware
CE: Datele companiei/ utilizatorilor
CUM: Atașament Spearphishing, execuție de script, injectare proces.
STRATEGIA: Amenințarea a început pe un computer fără antivirus și s-a răspândit lateral. Un proces de curatenie a fost efectuat de o firma specializata in IT&C.

RECUPERARE

IMPACT: Principalele consecințe ale atacului au fost următoarele:

☑ Pierderea datelor
☑ Întreruperea regulată a activității
☑ Compromisul sistemului
☑ Costuri financiare

STRATEGIA DE RECUPERARE: Strategia de recuperare a fost axată pe curățarea și reinstalarea computerelor compromise, curățarea și/sau reinițializarea căsuțelor de e-mail compromise.

O STRATEGIE MAI BUNĂ

☑ Instalați și păstrați un Antivirus/Antimalware actualizat
☑ Adoptați o prevenire a intruziunilor în rețea
☑ Restricționați conținutul bazat pe web
☑ Asigurați conștientizarea utilizatorului
☑ Politici de parole mai bune
☑ Managementul contului privilegiat
☑ Dezactivați sau eliminați caracteristica sau programul

- ☑ Prevenirea executării
- ☑ Audit
- ☑ Gestionarea contului utilizatorului
- ☑ Prevenirea comportamentului la punctul final
- ☑ Politici de utilizare a conturilor.

LECȚII ÎNVĂȚATE

Chiar dacă Emotet a fost distrus printr-o activitate concertată internațională, rămâne de văzut dacă acest lucru va avea un impact de lungă durată.

Este de remarcat că malware-urile folosesc aproape aceleași tehnici pentru a pătrunde și a se răspândi în sălbăticie, deci este obligatoriu să fii conștient și atent, deoarece atacurile cibernetice vor continua să existe în viitor. Măsuri precum luarea în considerare a comunicării cu lumea folosind un computer izolat de rețeaua care găzduiește infrastructura critică, utilizarea unor soluții de securitate capabile și actualizate, luarea în considerare a celor mai recente actualizări sunt unele care ar trebui prevăzute.

Phishing desemnează un termen umbrelă pentru atacuri de tip inginerie socială care sunt efectuate în prezent prin e-mailuri sau aplicații de rețele sociale.

STUDIU DE CAZ 11: DOBÂNDIREA ACCESULUI ILICIT LA CREDENȚIALE

ORGANIZAȚIA ȚINTĂ

Ca orice companie modernă, în cazul situației descrise, comunicațiile electronice prin internet cu clienții și furnizorii săi sunt cea mai preferată cale. În cadrul acestui tip de comunicare una dintre cele mai utilizate este e-mail-ul. Permite menținerea asincronă a contactului cu părțile interesate gestionate într-un mod eficient de mai mult de o persoană. Compania se află pe piață de peste jumătate de secol și în fiecare departament a fost puternic dezvoltată pe digitalizare, iar în acest context este inclus și departamentul de relații cu clienții. Pentru angajații afiliați a fost creat un grup de e-mail pentru gestionarea solicitărilor online de la computere dedicate protejate de antivirus și funcționalitate de filtrare a spam-ului pe serverul de e-mail.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile necesare descrierii acestui atac cibernetic au fost colectate printr-un interviu cu unul dintre tehnicienii TI ai companiei. Interacțiunea s-a realizat cu condiția păstrării în mod anonim a informațiilor sensibile. Chiar dacă intervievatul a fost dispus să descrie incidentul, unele informații nu au putut fi obținute deoarece problema a fost gestionată de o echipă diferită.

PREVENIRE

Deși au fost desfășurate campanii de conștientizare de către Direcția Națională de Securitate Cibernetică cu privire la măsurile care trebuie luate, potrivit rapoartelor existente, multe persoane publice, organizații private și persoane fizice au fost afectate.

Compania a impus utilizarea instrumentelor de securitate și reglementări personalizate în ceea ce privește munca online, dar acestea nu au fost suficiente din cauza experienței de bază în domeniul digital a unor angajați.

IDENTIFICARE

Phishing desemnează un termen umbrelă pentru un atac de tip inginerie socială care sunt efectuate în prezent prin e-mailuri sau aplicații de rețele sociale. De obicei, infractorii cibernetici trimit mesaje nesolicitate în vrac. Vor să vizeze cât mai mulți oameni, pentru a-i prinde pe unii dintre ei cu trucul lor.

Infractorii cibernetici încearcă să exploateze tendința unui fel de „oferte grozave" sau cu niște instrucțiuni administrative. Multe dintre aceste tipuri de mesaje par a fi legitime, deoarece folosesc aceeași identitate vizuală ca și companii, servicii sau aplicații online cunoscute. Unele exemple includ companii precum Google, Amazon, Microsoft, Yahoo, LinkedIn etc. sau servicii și aplicații bancare populare, cum ar fi cea de gestionare a e-mailului pe web.

Credibilitatea se dorește a fi obținută prin copierea schemei de culori, stilului, siglei și motto-urilor identității copiate. Sunt folosite linii de subiect tipice atractive.

Pe baza descrierii furnizate și a rapoartelor suplimentare din media, următoarele detalii au fost implicate în incidență:

- ☑ A fost primit un e-mail de phishing proiectat social care susținea necesitatea schimbării urgente a parolei de acces pentru a evita încetarea serviciului;
- ☑ Furnizarea de acreditări entității nelegitime a dus la accesul pe contul de e-mail și întreruperea accesului legitim prin schimbarea parolei;
- ☑ Contul compromis a fost folosit pentru mesaje de phishing nesolicitate trimise persoanelor de contact existente și altor adrese deținute de atacator;
- ☑ Din cauza mesajelor spam masive trimise pe Internet, serviciul de e-mail a fost inclus pe lista neagră, astfel încât funcționarea normală a fost întreruptă;
- ☑ Sistemul de e-mail a fost suspendat temporar pentru a opri spamurile suplimentare;
- ☑ Operațiunile online au fost afectate.

Conform cadrului MITRE ATT&CK, această incidență poate fi descrisă după cum urmează:

1. T1598.001 - Serviciul Spearphishing
2. T1598.002 - Atașament de spearphishing
3. T1598.003 - Link de spearphishing

RĂSPUNS

- ☑ **CINE:** Atacatorul nu a putut fi identificat cu precizie, deoarece au fost înregistrate origini din mai multe țări. A fost implicată o posibilă utilizare VPN.
- ☑ **PE CINE:** Fără țintă specifică
- ☑ **DE CE:** Colectare de date sensibile și extorcare de bani
- ☑ **CE:** Datele companiei/ utilizatorilor
- ☑ **CUM:** Phishing, furt de acreditări
- ☑ **STRATEGIA:** Amenințarea a început prin deschiderea unui e-mail uzurpat, accesarea link-urilor falsificate și trimiterea de date sensibile. Resetarea acreditărilor și eliminarea de pe lista neagră au fost efectuate de echipa TI.

RECUPERARE

IMPACT: Principalele consecințe ale atacului au fost următoarele:

- ☑ Pierderea acreditării
- ☑ Întreruperea regulată a activității
- ☑ Compromiterea sistemului.

STRATEGIA DE RECUPERARE: Strategia de recuperare a fost concentrată pe resetarea acreditărilor și curățarea clienților de e-mail compromis.

O STRATEGIE MAI BUNĂ

- ☑ Instalați și păstrați un sistem de filtrare Antivirus/Antimalware/E-mail actualizat
- ☑ Adoptați o prevenire a intruziunilor în rețea
- ☑ Restricționați conținutul bazat pe web
- ☑ Asigurați conștientizarea utilizatorului
- ☑ Politici de parole mai bune
- ☑ Managementul contului privilegiat
- ☑ Audit
- ☑ Gestionarea contului utilizatorului
- ☑ Prevenirea comportamentului la punct final
- ☑ Politici de utilizare a conturilor.

LECȚII ÎNVĂȚATE

Chiar dacă phishingul nu este o tehnică nouă, acesta rămâne una dintre principalele căi în multe atacuri de securitate cibernetică.

Este de remarcat că malware-urile folosesc această tehnică pentru a pătrunde și a se răspândi în sălbăticie, așa că este obligatoriu să fii conștient și atent, deoarece atacurile cibernetice în acest fel vor continua să existe. Măsuri precum luarea în considerare a utilizării unor servicii de e-mail protejate mai bine actualizate, mai multă conștientizare cu privire la accesarea e-mailurilor și analiza corectă a legitimității expeditorului.

STUDIU DE CAZ 12: APLICAȚII EXPRIRATE EXPUSE ONLINE

ORGANIZAȚIA ȚINTĂ

În zilele noastre, multe companii și-au schimbat modul de a-și furniza serviciile prin mutarea online. Este cazul exemplului dezafectat, unde la biroul de prestări servicii de tip financiar care operau din 1998 au fost migrate online de mai bine de un deceniu. Noua abordare a îmbunătățit activitatea generală a companiei și satisfacția clienților. Cu toate acestea, aceste realizări au fost posibile numai după un efort important de dezvoltare a software-ului personalizat, dezvoltat intern. Această aplicație online a permis clienților și angajaților să efectueze operațiunile necesare. Platforma furnizată dezvoltată în acea perioadă a fost menținut până când suportul a fost disponibil înainte de lansarea noii modificări majore. În timp, numărul de angajați a fost redus din cauza automatizării proceselor existente și a schimbărilor pieței. Upgrade-ul la noua versiune a fost amânat, deoarece au fost necesare investiții hardware și software.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile necesare pentru a descrie acest atac cibernetic au fost colectate printr-un interviu cu CEO-ul companiei. Interacțiunea s-a realizat cu condiția păstrării în mod anonim a informațiilor sensibile.

PREVENIRE

Deși au fost desfășurate campanii de conștientizare de către Direcția Națională de Securitate Cibernetică cu privire la măsurile care trebuie luate, multe organizații publice sau private ignoră sau întârzie decizia și acțiunile necesare pentru actualizarea sistemelor lor informatice.

Compania a impus utilizarea unor soluții de securitate cunoscute, firewall-uri, segmentare a rețelei etc. dar acestea nu au fost suficiente, deoarece a rămas o vulnerabilitate expusă într-unul dintre modulele software operate.

IDENTIFICARE

Atacurile de injecție în flux abuzează de capacitatea unei aplicații web online de a accepta conținut încărcat, cum ar fi diferite tipuri de documente sau fișiere de imagini. Folosind abordarea de includere a fișierelor de la distanță, un atacator poate exploata vulnerabilitatea din codul serverului pentru a accepta o adresă URL de pe alt site ca intrare validă. Această acțiune este apoi folosită pentru a executa codul atacatorului rău intenționat. În plus, includerea fișierelor locale poate fi

utilizată pentru a obține o aplicație web care să returneze conținutul dorit din sistemul de fișiere local.

Un exemplu popular este întâlnit în cazul framework-ului PHP utilizat de WordPress, permițând hackerului să acceseze fișierul de configurare. Acest atac poate permite, de asemenea, accesul la descărcarea oricăror fișiere de cod sursă PHP care rulează site-ul web, oferind noi posibilități pentru alte vulnerabilități de securitate. Versiunile PHP recente sunt protejate de includerea fișierelor de la distanță în mod implicit, dar dacă din greșeală includerea fișierelor locale este expusă, acest tip de atac este încă posibil.

Pe baza descrierii furnizate, a rapoartelor tehnice suplimentare, a buletinelor de securitate și vulnerabilități, în incident au fost implicate următoarele detalii:

- ☑ Printr-un atac de tip brute force, un cont protejat cu o parolă slabă este accesat nelegitim;
- ☑ Acreditările descoperite permit modificarea datelor asociate contului;
- ☑ Contul compromis a permis ca vulnerabilitatea de injectare a fluxului să fie expusă și execuția de cod nedorită pe server a fost folosită pentru a elimina jurnalele de istoric de acces;
- ☑ Din cauza execuției necontrolate a codului serverului, unele module ale aplicației devin inutilizabile și conduc la oprirea serviciului, astfel încât funcționarea normală a fost întreruptă;
- ☑ Sistemul a fost deconectat temporar de la Internet pentru investigații ulterioare legate de funcționarea defectuoasă a aplicației web;
- ☑ Operațiunile online au fost afectate.

Conform cadrului MITRE ATT&CK, această incidență poate fi descrisă după cum urmează:

1. T1110.001 - Ghicirea parolei
2. T1078 - Acces la conturi valide
3. T1518 - Descoperirea software-ului
4. T1082 - Descoperirea informațiilor de sistem
5. T1007 - Descoperirea serviciului de sistem
6. T0826 Pierderea disponibilității.

RĂSPUNS

- ☑ **CINE:** Atacatorul nu a putut fi identificat cu precizie.
- ☑ **PE CINE:** Fără țintă specifică
- ☑ **DE CE:** Colectarea datelor sensibile și refuzul serviciului
- ☑ **CE:** Datele companiei/ utilizatorilor
- ☑ **CUM:** Atacul de forță brută, furtul de acreditări și execuția codului prin injectare în flux.

☑ **STRATEGIA:** Amenințarea a început printr-un atac de forță brută care a dus la o descoperire slabă a acreditărilor, exploatând vulnerabilitatea într-un modul software care nu este accesibil publicului și apoi execuția neautorizată a codului. Strategia slabă de protecție a accesului online, modulul software învechit și codul neîntreținut sunt cauza principală a incidenței.

RECUPERARE

IMPACT: Principalele consecințe ale atacului au fost următoarele:

☑ Pierderea acreditării
☑ Compromiterea sistemului
☑ Întreruperea regulată a activității.

STRATEGIA DE RECUPERARE: Strategia de recuperare s-a concentrat pe actualizarea majoră a platformei, rescrierea unei părți importante a codului.

O STRATEGIE MAI BUNĂ

☑ Instalați și păstrați un software actualizat
☑ Aplicați politica privind parolele puternice
☑ Politici de utilizare a conturilor
☑ Adoptarea mecanismului de autentificare cu doi factori
☑ Adoptați o prevenire a intruziunilor în rețea
☑ Restricționați accesul de la distanță
☑ Asigurați conștientizarea utilizatorului
☑ Implementarea unui audit de securitate periodic
☑ Gestionarea contului utilizatorului
☑ Prevenirea comportamentului la punct final.

LECȚII ÎNVĂȚATE

Chiar dacă se știe că software-ul învechit care rulează este predispus la vulnerabilități de securitate, acesta rămâne una dintre principalele căi în multe atacuri de securitate cibernetică.

Aplicațiile web fiind accesibile în întreaga lume sunt expuse la multe vulnerabilități și, în consecință, necesită o atenție specială din multe perspective.

Măsuri precum luarea în considerare a actualizării constante a software-ului, îmbunătățiri și adoptarea de noi tehnici și soluții pentru mecanismele de autentificare, adoptarea unui proces de audit regulat sunt câteva dintre măsurile comune care pot fi luate în considerare.

STUDIU DE CAZ 13: RISCURILE UNUI ATAC EFECTUAT DE UN FOST ANGAJAT

ORGANIZAȚIA ȚINTĂ

Organizația în care s-a produs atacul cibernetic, acționează pe urmărire comercială, într-o ramură de automobile, cu aproximativ 2000 de angajați. Este situată în statul Paraná și Santa Catarina din Brazilia.

Atacul cibernetic a vizat zona tehnologiei informației, datorită cunoștințelor pe care hackerul le avea de la fostul angajat al organizației, oferindu-i avantajul de a convinge sistemul.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile din acest studiu de caz se bazează pe un studiu despre riscurile unui atac cibernetic condus de un fost angajat. Studiul de caz este realizat din punctul de vedere al organizației care a suferit atacul cibernetic.

Obiectivul general al acestui studiu de caz este acela de a demonstra importanța pe care companiile trebuie să o acorde în legătură cu ingineria socială în mediile lor, pentru a evita invaziile și/sau fraudele cauzate de imprudența sau asistența neintenționată a angajaților ca încălcări ale muncii de hacker.

PREVENIRE

Pentru a preveni eventualele daune, compania deținea deja un departament TI care gestiona firewall-uri, instrumente de scurgere de informații și criptarea datelor.

IDENTIFICARE

În acest studiu de caz, amprenta a început cu diverse vizite pe pagina web a asociației, cu intenția de a înțelege dinamica acestora, afacerile și în special mărcile lor (având în vedere că atacatorul a direcționat căutarea unor date pe care hackerul nu le cunoștea încă). Când colecatrea a început și informațiile interne și specifice ale organizației sunt în posesia atacatorului, acesta a continuat cu conexiunile la unul dintre magazinele din lanț pentru a descoperi numele managerilor și ale persoanelor care ar putea avea acces privilegiat în cadrul organizației.

Pentru a face acest lucru, atacatorul s-a pozat, prin telefon, ca un client care avea probleme legale cu firma. Pentru a rezolva aceasta problema, firma ar fi sunat clientul și l-ar fi rugat să discute cu managerul magazinului în cauză, în condițiile în care acesta ar fi persoana cea mai în măsură să

răspundă într-o astfel de situație. Datorită acestei interacțiuni s-a obținut ușor, numele managerului, locația unde a lucrat și numărul de telefon.

După acest apel telefonic, s-a încercat contactarea managerului pe canalele informate pentru a verifica informațiile colectate. Resetarea parolei s-a făcut la contactarea departamentului TI, dându-se drept angajatul însuși, pentru ca departamentul să-l informeze despre datele de acces ale utilizatorului.

Folosind puțină persuasiune și argumentul că datele pentru placă depind de acest acces, în cele din urmă tehnicianul a resetat parola și a informat prin telefon noua parolă. Mai mult decât atât, a fost posibil să-l convingă să configureze accesul VPN (tehnologie pentru acces la distanță în mediul companiei) astfel încât utilizatorul ipotetic să poată lucra din afara biroului

RĂSPUNS

CINE: Atacatorul era un fost angajat.
PE CINE: O organizație care lucrează pe urmărire comercială, în ramura auto.
DE CE: Atacul a vizat organizația din motive necunoscute.
CE: Proprietatea vizată a fost sectorul tehnologiei informației pentru a colecta informații privilegiate ale organizației și date personale ale actualilor angajați.

CUM: Atacul a început cu obținerea numelui managerului unui magazin, a continuat să contacteze sectorul de tehnologie a informației al companiei și i-a convins să reseteze parola. Așa fostul angajat s-a prefăcut a fi manager și a avut acces la tot ce ține de informațiile privilegiate, datele personale ale angajaților și clienților și orice dorește hackerul.

RECUPERARE

Compania a început să-i instruiască pe colaboratori să acorde atenție tipurilor de informații pe care de obicei le transmit terților, mai ales dacă este vorba de informații critice. Niciodată, sub nicio circumstanță, un angajat nu ar trebui să transmită prin telefon informații esențiale, cum ar fi parolele. Acestea trebuie furnizate părților interesate prin metode sigure, cum ar fi scrisorile recomandate sau prin intermediul managerului responsabil.

Oferiți, de asemenea, instruire pentru a-i face pe angajați să conștientizeze că sunt atenți la informațiile pe care le distribuie pe internet. Instruirea trebuie axată pe riscurile pe care informațiile partajate le pot aduce ocupației lor, dar și vieții personale, cum ar fi răpiri, detalii de viață și securitatea personală.

Această companie este conștientă că trebuie să ofere condiții tehnice și fizice pentru aplicarea bunelor practici de securitate, dar, mai presus de toate, să pună în valoare și să încurajeze adoptarea de bune practici și protocoale de securitate mai stricte de către angajații săi, fie într-un mediu

corporativ sau personal pentru a controla, în cel mai bun mod posibil, cel mai slab factor al securității informației: factorul uman.

LECȚII ÎNVĂȚATE

Organizația ar trebui să stabilească informațiile într-o procedură tip model simplă care poate frustra hackerul. Această procedură are 3 etape:

☑ **Public:** Informații care ar putea fi oferite oricui, de exemplu, contacte comerciale și corporații specifice, informații între clienți și afacerile corporației;

☑ **Privat:** Informații care nu pot fi oferite niciunei persoane și care privesc doar mediul corporativ. Sunt acoperite în această categorie informațiile referitoare la procedurile interne, datele corporative administrative și aspectele strategice ale companiei;

☑ **Confidențial:** Informații și date care nu ar trebui partajate în interiorul și în afara companiei, cum ar fi datele de înregistrare a angajaților, compensații, rezultatele sectoarelor și acțiunile strategice care privesc doar direcțiunea sau conducerea.

De asemenea, organizațiile ar trebui să aibă proceduri interne pentru a le proteja de atacurile de inginerie socială. Operatorii trebuie să fie bine instruiți cu privire la procesele pe care trebuie să le urmeze și la acțiunile pe care trebuie să le întreprindă în situațiile în care compania se simte atacată, cum ar fi transferul apelului către o persoană instruită să gestioneze acest tip de situație. Acțiunile simple pot duce la eșecul atacului. Imediat se poate spune că o listă de verificare inițială pentru a confirma datele solicitantului ar îngreuna accesul hackerului. Având în vedere că datele personale nu sunt ceva foarte greu de obținut, tehnicienii ar putea adopta un proces de returnare a contactului la numărul de telefon înregistrat al angajatului, pentru a confirma ca este vorba de fapt de angajatul în cauză.

STUDIU DE CAZ 14: ATACURILE CIBERNICE CA O NOUĂ REȘEDINȚĂ A PROVOCĂRILOR DE SECURITATE

ORGANIZAȚIA ȚINTĂ

Entitățile guvernamentale portugheze (în special Ministerul Administrației Interne), Forțele de Securitate și marile companii.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile pentru acest studiu de caz au fost culese printr-o cercetare de birou care se referă la o teză de master, unde autorul aplică un studiu și mai multe interviuri exploratorii cu specialiști și persoane responsabile de forțele de securitate naționale, pentru a concluziona dacă fenomenul hacktivista reprezintă o amenințare la adresa forțelor de securitate portugheze.

PREVENIRE

Pentru a preveni atacurile, unul dintre pașii pe care îi face echipa IT responsabilă cu securitatea cibernetică din aceste organizații este să monitorizeze canalele sociale, de exemplu: IRC-uri (Internet Relay Chat), tot felul de chat-uri, Facebook-uri, tot ceea ce este posibil să obțină informații de pe internet, fac și o urmărire și încearcă să vadă dacă există acțiuni suspecte.

Potrivit „modus operandi”, definit de termenii grupului Anonymous (Portugalia), ei fac publicitate inițial pe rețelele de socializare (IRC-uri și Facebook-uri), acțiunile pe care le vor întreprinde și atunci încep să comunice între ei. Apoi folosesc canale private de chat pentru a comunica între ei, ceea ce a dus la implementarea SOC (Security Operations Center) al MIA (Ministerul Administrației Interne), pentru a se pregăti pentru acest tip de atacuri.

IDENTIFICARE

Consecințele acestor atacuri au variat, în funcție de tipul de atac. Mulți au avut de-a face cu un atac de tip denial-of-service, (DOS, DDOS), care provoacă o epuizare a resurselor în ceea ce privește sistemele sau comunicațiile. De asemenea, s-au ocupat de unele tipuri de tentative de atacuri de intruziune, cum ar fi SQL Injection și defacements. Pescuitul prin e-mail, este și unul dintre cele mai frecvente atacuri, ducând uneori la acces la informații private.

În noiembrie 2011, a avut loc un atac pe site-ul sindicatului național pentru cariera șefilor PSP, cu dezvăluirea de date personale și confidențiale (brevete, numere de telefon și adrese de e-mail) a 107 angajați PSP.

“Atacurile DDoS au crescut constant ca frecvență în ultimii ani. Potrivit unui raport de la Cloudflare, atacurile DDoS cu răscumpărare au crescut cu aproape o treime între 2020 și 2021 și au crescut cu 75% în T4 2021, comparativ cu ultimele trei luni.” (Cook, 2022)

RĂSPUNS

Un atac asupra Poliției de Securitate Publică a fost asumat de grupul LulzSec Portugalia. Grupul portughez Anonymous a revendicat mai multe atacuri asupra site-urilor web guvernamentale și a instituțiilor relevante. În general, profilul hackerului este al unui tânăr, de vârstă școlară, la nivel secundar (clasa a X-a până la a XII-a). Poate exista una sau alta dintre situațiile în care sunt deja mai mulți adulți, poate cu mai puține cunoștințe în domeniul tehnologic, dar nemulțumiți de societate.

Acest tip de atac este disponibil oricărui cetățean. Este nevoie doar de persoana care caută pe internet instrumente, metode și grupuri și începe să participe. Aceste grupuri de persoane anonime, la momentul atacurilor, au desfășurat ateliere despre cum să faci un atac, cursuri „abc" despre cum să înțelegem atacul. Acestea oferă instrumente deja dezvoltate și pe care oricine le poate accesa de pe site, fiind necesar doar să introduceți adresa de destinație și o aplicație dezvoltă atacul.

Majoritatea atacatorilor, adică tinerii încă la școală, folosesc instrumente care sunt folosite de mulți specialiști, iar acei specialiști sunt oameni cu o diplomă academică mai avansată și mai în vârstă, care folosesc instrumente deja dezvoltate în scopul atacului cibernetic. Adică, pe internet, este posibil să căutați și să obțineți informații pentru a efectua atacul, cum să îl faceți și ce fel de instrumente sunt folosite pentru a ajuta la efectuarea atacului.

Atacul efectuat de LulzSec Portugalia a fost justificat pe Twitter susținând că este răspuns la acțiunea agenților provocatori care s-au infiltrat într-o demonstrație organizată de aceștia.

Dar de cele mai multe ori aceste atacuri se întâmplă pentru că acești oameni caută vizibilitate sau pun în pericol organizațiile, deoarece aceasta are adesea legătură cu nemulțumirea oamenilor față de contextul actual în care trăiesc cetățenii portughezi, iar oamenii își demonstrează adesea nemulțumirea în acest fel. Alteori este doar o glumă pentru atacatorii, cu vârste între 16 sau 17 ani, care nu au prea multe preocupări în plan social, de multe ori pentru că o fac prietenii și pentru a se promova în cadrul grupului de prieteni, iar alteori acestea sunt experiențe pe care le fac pentru că este epoca experimentării lucrurilor noi. De cele mai multe ori nu realizează impactul pe care îl pot avea aceste atacuri.

Totul începe cu un grup de hackeri care au cunoștințele tehnice și dezvoltă instrumente pentru a fi folosite de grupuri de oameni care nu au aceleași cunoștințe, ceea ce face procesul de hacking ușor pentru oricine.

O caracteristică a grupurilor portugheze este să atace site-urile web neprotejate și să exploateze vulnerabilitățile. Ei planifică atacuri asupra IRC-urilor (Internet Relay Chat) și a camerelor de chat, nu își asumă identitatea și folosesc porecle. Hacktiviștii portughezi folosesc instrumentele disponibile online pentru a efectua atacurile, adică „nu fabrică programe personalizate, ci le folosesc pe cele care sunt disponibile în rețea". În ceea ce privește persoanele care preiau organizarea și conducerea acestui tip de inițiative, acestea sunt adesea persoane cu puțină expertiză tehnică, dedicându-se să facă anunțuri și diseminări ale acțiunilor ce urmează a fi dezvoltate și adesea „cei care au chiar și abilități tehnice foarte specializate, habar nu au că sunt cei mai competenți și specializați din grup, cred că sunt oameni care știu puțin și că doar îi ajută pe alții care știu mai multe".

Grupul Anonymous folosește metode convenționale de hacking precum Havij114 și SQL Injection, principala sa inovație fiind crearea de site-uri web care efectuează atacuri DoS.

RECUPERARE

Consecințele posibile sunt furtul de informații, indisponibilitatea serviciilor și deformarea site-ului unde se fac modificări în informații, deoarece hackerii uneori elimină informații și le pot adăuga și ei.

Aceste atacuri pot pune în pericol încrederea acordată de cetățeni în instituțiile care sunt victime ale acestor grupuri dar și identificarea vulnerabilităților, iar influența altor persoane cu anumite idealuri sunt situații care pot să apară.

Aceste tipuri de atacuri evoluează, tehnicile se îmbunătățesc în timp, iar organizațiile trebuie să se adapteze și să evolueze pentru protecția rețelei sale. Aceștia au fost forțați să nu mai acceseze rețeaua până la îndeplinirea condițiilor pentru a asigura menținerea securității informațiilor interne. Și au făcut aceasta, în total, cel mult timp de o oră. Ocazional, unele servicii au fost pe timpul nopții inaccesibile.

S-a înființat CNCseg (Centrul Național de Securitate Cibernetică), care are mai mult de-a face cu problema apărării naționale, decât actualul Centrul de Apărare Cibernetică, care este de competența Ministerului Apărării Naționale, a cărui acțiune principală este atacul asupra hackerilor care pot dezvolta atacuri, efectuând detectarea și contraatacul acestor elemente.

MIA va participa, cel puțin la CNCseg, lucrează împreună cu GNS, care este entitatea care are această competență și va fi unul dintre inputurile informaționale pentru acest tip de securitate cibernetică. Ideea este ca acest centru să aibă informații despre ceea ce se întâmplă la nivel național, iar obiectivul este de a colecta informații atât de la centrele tehnologice ale administrației publice, bancare, industrie, diferitele domenii ale societății portugheze și, cu aceasta, să aibă o idee despre impactul și sfera de aplicare care poate avea un anumit tip de atac.

LECȚII ÎNVĂȚATE

Hacktivismul este văzut ca o nouă provocare pentru instituții și, mai ales, în cazul Forțelor de Securitate, un atac hacktivist poate provoca consecințe dăunătoare, care chiar pot influența îndeplinirea misiunilor acestora, fiind deci considerat o amenințare reală, în sensul că aceasta se caracterizează prin contrazicerea obiectivelor organizației, producând, de regulă, prejudicii materiale și/sau morale.

Capacitatea grupurilor hacktiviști de a efectua un atac este de obicei scăzută, deoarece folosesc instrumente disponibile în rețea și nu sunt foarte inovatoare în materie de hacking, profitând de exploatarea vulnerabilităților existente. În ceea ce privește oportunitatea, oricine de la un computer cu acces la rețea și cu anumite cunoștințe sau dorință de a învăța din informațiile disponibile în rețea este capabil să dezvolte un atac cibernetic, iar acest fapt devine îngrijorător pentru forțele de securitate.

În ceea ce privește securitatea computerelor, se spune adesea că nu există siguranță totală și nu există sisteme 100% sigure, așa că guvernul și Portugalia nu fac excepție. Ceea ce s-a asistat este crearea unui set de infrastructuri care să permită o structură de securitate care să corespundă și să răspundă acestui tip de fenomen: CNCseg-ul recent creat, realizat de PJ pentru a lupta împotriva criminalității informatice. Educarea oamenilor este cu siguranță ceva care îi va provoca pe toți să realizeze că folosim și noi tehnologii, platforme de internet și alte rețele care au puterea de a schimba siguranța cetățenilor săi.

Consecințele unui atac hacktivist asupra forțelor naționale de securitate:

- ☑ Direct: consecințe economice, sociale, politice și de securitate.
- ☑ Indirect: sentimentul de securitate, de reglementare socială și, în cele din urmă, suveranitatea țării, instituțiilor și familiilor.

"Ransomware-ul va costa victimele peste 265 de miliarde de dolari anual până în 2031." (Întreprinderi de securitate cibernetică).

STUDIU DE CAZ 15: „EPOCA DE AUR" A „RANSOMWARE". CUM SĂ PREVENIȚI ȘI SĂ TRATAȚI CU UN HIJACK DE DATE

ORGANIZAȚIA ȚINTĂ

Majoritatea companiilor portugheze sunt în „generația 3" de securitate cibernetică, iar atacurile sunt în „generația 6". În acest studiu de caz aflăm cum să procedăm pentru a preveni atacurile ransomware precum cel cu care se confruntă grupul IMPRESA, din ce în ce mai frecvent.

IMPRESA este cel mai mare grup de media portughez, care operează în trei domenii de activitate - print, digital și televiziune.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile pentru acest studiu de caz au fost obținute printr-un articol de știri despre prevenirea ransomware-urilor, care include interviul lui Rui Duro, expert în securitate cibernetică.

PREVENIRE

Vremurile pandemiei au facilitat creșterea acestui tip de atac ransomware. Pe de o parte, lucrul la domiciliu, ceea ce duce la dispersarea sistemelor și crește riscul. Pe de altă parte, din ce în ce mai multe aplicații migrează către sistemele în „cloud".

„Acest lucru are mai multe riscuri asociate", spune Rui Duro. Sistemele sunt acum „în alt furnizor de servicii" și este necesar „să cumpărați tehnologie și pentru cloud, deoarece nu este sigură în sine". Pentru specialist, „această

evoluție către „clOud” a fost adesea mai rapidă decât evoluția cunoștințelor angajaților din tehnologia informației”.

Pe de altă parte, multe companii au fost depășite de sofisticarea atacurilor. „Noi (grupul IMPRESA) suntem în generația a 6-a de atacuri și majoritatea companiilor sunt încă în generația a 3-a, într-un stadiu foarte incipient de protecție dată fiind evoluția atacurilor. Mentalitatea trebuie să se schimbe, trebuie să existe un buget și resurse pentru a se adapta la această nouă realitate”, explică Rui Duro.

IDENTIFICARE

Pe paginile site-urilor grupului apare un mesaj asemănător cu cel primit de SIC (canal tv portughez): „Datele interne ale sistemelor au fost copiate și șterse. 50 TB de date sunt în mâinile noastre. Contactează-ne dacă vrei datele înapoi”.

Rui Duro explică că „de obicei, ransomware-ul apare în companii prin ceea ce numim plasarea unei ‘sarcini utile‘ inițiale în cadrul companiei”.

Acest lucru se întâmplă în moduri diferite, cum ar fi printr-un atac de tip phishing asupra unui element al companiei. Alteori, cineva de la companie „descărcă” din neatenție malware-ul. Există încă o a treia cale, când actorii au scopul de a ataca o anumită companie și caută vulnerabilități - acesta este un „atac țintă”.

După ce malware-ul inițial este în interiorul companiei, acesta descarcă un al doilea malware, care execută ransomware-ul. Apoi începe să facă o „scanare”, căutând servere și alte sisteme. Scopul este de a face un profit cât mai mare – potrivit expertului, pentru infractori „nu are rost să cripteze un computer sau două, ideea este să cripteze cât mai multe computere și de preferat pe cele vitale”.

Hackerii instalează apoi malware-ul pe cât mai multe sisteme posibil, dar nu criptează datele imediat. De obicei, „se lasă câteva săptămâni, uneori mai mult”.

Cei care atacă știu că una dintre modalitățile prin care companiile își recuperează datele este prin backup - așa că se așteaptă să existe o copie de rezervă și, de îndată ce este restaurată, apare din nou o infecție.

Atunci când are loc criptarea, criminalii pun presiune asupra companiilor, de obicei pentru a cere o răscumpărare în numerar – de obicei în criptomonede.

RĂSPUNS

La două zile după ce grupul de hacking „Lapsus$ Group” a atacat site-urile grupului Impresa, site-urile erau încă indisponibile.

Poliția Judiciară din Portugalia a confirmat că investighează cazul, împreună cu Centrul Național de Securitate Cibernetică (CNCS), așa cum a comunicat deja grupul media.

Această întârziere în resetarea sistemelor este comună în atacuri ca acesta. Potrivit lui Rui Duro, responsabil pentru Check Point Software în Portugalia, „timpul necesar pentru a face față acestor atacuri variază foarte mult. Depinde foarte mult de mărimea companiei, de atac, de capacitatea companiei în materie de tehnologii informaționale (TI) și de cât de pregătită a fost compania să înlocuiască sistemele. Într-o companie mică, uneori durează o zi sau două, dacă este o companie mare, poate dura chiar câteva săptămâni și uneori poate presupune refacerea unei întregi infrastructuri”.

Atacul ransomware a devenit deja o amenințare reală și imediată pentru companiile din întreaga lume - iar Portugalia nu face excepție. Pentru Agenția Europeană de Securitate Cibernetică (ENISA), pandemia a adus cu ea o „epoca de aur" pentru infractorii cibernetici.

Potrivit agenției, între aprilie 2020 și iulie 2021, a existat o creștere cu 150% a atacurilor înregistrate.

În Portugalia, încă nu există date oficiale cu privire la ultimul an, dar în raportul anual de securitate internă, pentru 2020, ransomware-ul este deja identificat drept „cea mai comună formă de sabotaj informatic, menținând rate ridicate de cazuri și afectând mai ales instituțiile Guvernului și întreprinderile mici și mijlocii".

Potrivit acestui raport, atacurile cibernetice s-au dublat în Portugalia din 2019 (754 de incidente) până în 2020 (1418 incidente). În domeniul Securității Informaționale, unde atacurile ransomware sunt predominante, în 2020 au fost de aproximativ 10 ori mai multe incidente decât în 2019. Rui Duro, șeful Check Point Software din Portugalia, explică că „90 până la 95% din cazuri nu sunt raportate sau cunoscute. Companiile ajung să-și revină prin backup-uri și nu raportează atacuri".

Potrivit datelor dintr-un studiu publicat de compania pe care o conduce, care creează soluții de securitate tehnologică pentru cele mai mari companii din lume, organizațiile portugheze suferă în medie 947 de atacuri malware pe săptămână, un număr mai mare decât media globală de 870 de atacuri. Aproximativ 90% dintre fișierele rău intenționate ajung prin e-mail.

Datele de la Check Point Software arată, de asemenea, că în decembrie 2021, atacurile ransomware au ajuns la peste 2,5% dintre companiile portugheze.

RECUPERARE

Un ransomware este o formă de malware (combinație a cuvintelor englezești „malicious" și „software") concepută pentru a cripta serverele și zonele de stocare ale computerelor.

De obicei, „hackerii" din spatele atacului afișează mesaje care cer plata unei sume pentru a decripta sistemul și a-l returna proprietarului. Potrivit expertului în securitate cibernetică, atacurile ransomware sunt din ce în ce mai sofisticate, iar piraților sunt văzuți din ce în ce mai mult încercând să „dubleze sau să tripleze extorcarea".

În dublă extorcare, „în perioada în care malware-ul așteaptă backup, ei copiază date semnificative din baze de date, servere de e-mail, servere financiare, încearcă să caute date sensibile și exportă cantități uriașe de date. Ei spun că nu merită să încerci să recuperezi serviciul cu copii de rezervă, pentru că au datele ostatice".

În cazul triplei extorcări, cu datele sensibile în posesia lor, piraților amenință că vor viza clienții și furnizorii companiei dacă compania nu plătește răscumpărarea.

LECȚII ÎNVĂȚATE

Pentru a preveni un atac, este necesar să schimbați mentalitățile și să presupuneți că se va întâmpla. Pentru expertul în securitate cibernetică, acesta este cel mai important lucru „Am mai bine de 30 de ani pe piață de lucru în acest domeniu, am început când atacurile erau o glumă, față de ceea ce sunt astăzi, dar și astăzi văd factorii de decizie gândindu-se că încă nu este îngrijorător, nu sunt relevante și că lor nu li se va întâmpla. Primul pas este schimbarea acestei mentalități. Se poate întâmpla oricui, iar cu puțin timp în urmă s-a întâmplat cu EDP. Când se întâmplă, trebuie să fiu pregătit pentru asta". Luați în serios cei trei piloni ai securității cibernetice: oameni, procese și tehnologie.

a) Oameni

„Adesea, chiar și companiile care iau în serios securitatea cibernetică se concentrează prea mult pe tehnologie ca modalitate de a se proteja și uită că este necesar să instruiască oamenii să se comporte în siguranță”, spune expertul.

b) Procese

„Este important să existe un proces de recuperare în urma dezastrului, de a gestiona și califica informațiile, de a avea un proces de backup eficient, de a avea depozite de informații. Multe companii nu sunt pregătite, iar primele ore sunt un haos complet, pentru că nu au fost atenți să pregătească procesul de recuperare”, dezvăluie el.

c) Tehnologie

„Folosirea tehnologiei potrivite realității pe care o avem astăzi. Multe companii cumpără tehnologie și este ceea ce eu numesc cumpărarea unui „fals sentiment de securitate” - cumpără tehnologie, dar aceasta nu mai este adecvată realității pe care o avem astăzi. Cumpără firewall-ul tradițional, în locul unui punct final avansat care evită criptarea sistemelor și care folosește un punct final simplu, care detectează unele programe malware, dar nu împiedică aceste criptări".

Specialistul amintește că, în aceste cazuri, „panica nu ajută cu nimic”. În aceste situații, este necesar să se informeze autoritățile să nu plătească niciodată răscumpărarea, deoarece aceasta este la fel cu perpetuarea infracțiunii, a spune infractorilor că merită. Unul dintre procesele pe care companiile trebuie să le dezvolte în prealabil, pentru specialiști, este cum să-și revină după un astfel de atac, astfel încât să existe acel calm și ca fiecare să-și cunoască rolul în acest proces.

STUDIU DE CAZ 16: MALWARE/ KEYLOGGER

ORGANIZAȚIA ȚINTĂ

O mică companie de producție deținută de familie a folosit pe scară largă serviciile bancare online. Angajatul contabil s-a autentificat la sistemul online banking cu o companie, un ID și o parolă specifice utilizatorului. A trebuit să se răspundă la două întrebări provocatoare pentru tranzacțiile de peste 1.000 EUR.

Proprietarul a fost anunțat că un transfer de plată de 5.000 de euro a fost inițiat de la o sursă necunoscută. Ei au contactat banca și au identificat că în doar o săptămână infractorii cibernetici au efectuat zece transferuri din conturile bancare ale companiei, în valoare totală de 10.000 de euro. Cum? Unul dintre angajații lor deschisese un e-mail de la ceea ce credea că este un furnizor de materiale, dar era, în schimb, un e-mail rău intenționat cu malware dintr-un cont de impostor.

Atacatorii au reușit să instaleze programe malware în computerele companiei, folosind un keylogger pentru a captura acreditările bancare. Un keylogger este un software care monitorizează în tăcere apăsările de taste ale computerului și trimite informațiile unui criminal cibernetic. Apoi pot accesa online servicii bancare și alte servicii financiare, folosind numere de cont și parole valide.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile pentru acest atac cibernetic au fost colectate prin două interviuri, unul cu proprietarul companiei și unul cu un tehnician al companiei de suport TI. Ambii au fost dispuși să descrie și să dea detalii despre incident, dar au cerut să păstreze anonimitatea ambelor companii, deoarece informațiile erau prea sensibile pentru ei.

PREVENIRE

În compania analizată, procedurile și mecanismele de securitate cibernetică au fost identificate ca nesatisfăcătoare. Deși computerele companiei aveau software antivirus, nimeni nu a fost actualizat. În plus, nu s-au desfășurat campanii de conștientizare și unii angajați păreau să aibă o înțelegere limitată a riscurilor cibernetice.

Un keylogger este un software care monitorizează în tăcere apăsările de taste ale computerului și trimite informațiile unui criminal cibernetic.

IDENTIFICARE

Pe baza informațiilor furnizate au fost culese următoarele detalii despre incidență:

☑ A fost primit un e-mail de phishing proiectat social, cu un fișier comprimat arhivat atașat ca verificare la o comandă de furnizor.
☑ Deschizând fișierul, malware-ul a fost instalat pe computer.
☑ A fost instalat un software de înregistrare a tastelor care monitorizează în tăcere apăsările de taste ale computerului și trimite informațiile unui criminal cibernetic.
☑ Apoi, criminalul cibernetic folosește acreditările capturate pentru a accesa contul bancar și a efectuat transferul folosind numere de cont și parole valide.
☑ Incidentul a fost identificat doar atunci când infractorul cibernetic a încercat să facă un transfer mai mare de 1000 €.

RĂSPUNS

Neavând un plan de securitate cibernetică în vigoare, răspunsul companiei la atac a fost întârziat.

CINE: Atacatorul nu a putut fi identificat cu precizie. Se cunoștea doar o adresă de e-mail și originea posibilă.
PE CINE: Fără țintă specifică.
DE CE: Colectarea datelor sensibile și utilizarea acestora pentru a fura bani
CE: Acreditările contului bancar al companiei.
CUM: Keylogger, monitorizează în tăcere apăsările de taste ale computerului.

STRATEGIA: Amenințarea a început pe un computer fără antivirus. A fost efectuat Un proces de curățare de către expertul TIC al unei companii. Contul bancar s-a închis și acreditările s-au schimbat. Compania TIC i-a ajutat să finalizeze o revizuire completă a securității cibernetice a sistemelor lor și să identifice care a fost sursa incidentului. Ei recomandă, de asemenea, upgrade la software-ul lor de securitate.

RECUPERARE

IMPACT: Compania și-a închis contul bancar și a demarat acțiuni legale pentru a-și recupera pierderile. Afacerea a recuperat o mică parte din pierderi. Nu s-au recuperat bani pentru timp și taxe legale.

RECUPERARE: Strategia de recuperare a fost axată pe închiderea contului bancar pentru a evita alte pierderi. Alte acțiuni au fost, curățarea computerului compromis și a căsuței poștale electronice compromise. Au verificat toate computerele companiei pentru orice alt atac.

STRATEGIA: Compania ar trebui să implementeze diverse acțiuni pentru a preveni astfel de incidente. Strategia sa trebuie să se concentreze pe următoarele acțiuni/pași:

- ☑ Implementarea de politici de securitate, cum ar fi Politica de modificare a parolei și Politica de gestionare a utilizatorilor contului.
- ☑ Instalarea și menținerea unui software antivirus/antimalware actualizat.
- ☑ Efectuarea de programe de instruire pentru a asigura gradul de conștientizare a angajaților.
- ☑ Restricționarea conținutului bazat pe web.
- ☑ Efectuarea de controale și audituri regulate.
- ☑ Să efectueze prevenirea şi implementarea unui sistem de management al riscurilor.

LECȚII ÎNVĂȚATE

- ☑ Notificări - configurați alerte de tranzacție pe toate cardurile de credit, debit și conturile bancare.
- ☑ Controlul accesului. Restricționați accesul la conturile sensibile doar acelor angajați care au nevoie de acces; schimbați frecvent parolele.
- ☑ Compania ar trebui să-și evalueze riscul și să evalueze opțiunile de asigurare de răspundere cibernetică.
- ☑ Alegeți bănci care oferă mai multe straturi de autentificare pentru a accesa conturi și tranzacții.
- ☑ Creați, mențineți și practicați un plan de răspuns la incidente cibernetice care poate fi implementat rapid.
- ☑ Infractorii cibernetici livrează și instalează software rău intenționat prin e-mail. Instruiți angajații cu privire la securitatea e-mailului.

STUDIU DE CAZ 17: UN CALCULATOR FURAT PROVOCĂ ÎNCĂLCAREA GRAVĂ A DATELOR

ORGANIZAȚIA ȚINTĂ

O companie de consultanță formată din 10 persoane a trimis o echipă mică în Ungaria pentru a finaliza un proiect pentru clienți. În timpul șederii lor, consultantul senior și-a lăsat laptopul eliberat de serviciu, care avea acces la informații sensibile ale clienților și detalii bancare ale companiei, într-o mașină încuiată în timp ce lucra. Mașina a fost spartă, iar laptopul a fost furat. Din păcate, datele de pe computer au fost necriptate deoarece angajatul nu a aplicat politica companiei de a cripta toate

datele sensibile de pe computerul său. Compania se temea acum de un atac cibernetic asupra sistemelor sale, a conturilor bancare și a scurgerilor de date despre clienți.

Tipul de atac: Furtul fizic al unui computer necriptat. Criptarea este procesul de amestecare a textului care poate fi citit, astfel încât să poată fi citit doar de persoana care deține cheia de decriptare. Acesta creează un nivel suplimentar de securitate pentru informațiile sensibile.

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile necesare descrierii incidentului au fost colectate printr-un interviu cu consultantul senior al companiei și tehnicianul TI al companiei TIC care sprijină firma de consultanță. Interacțiunea s-a realizat cu condiția păstrării în mod anonim a informațiilor sensibile. Chiar dacă intervievatul a fost dispus să descrie incidentul, unele informații de criptare nu au putut fi obținute și acesta este motivul pentru care s-a solicitat companiei TIC suport să lămurească cazul.

PREVENIRE

Deși incidentul nu este un incident clar de atac cibernetic, este un incident grav și foarte frecvent care provoacă o serie de atacuri cibernetice semnificative.

În cazul companiei analizate, din perspectiva securității cibernetice au funcționat politici și mecanisme specifice, dar acestea nu au fost implementate de unii angajați din cauza experienței reduse în domeniul informațiilor și al riscurilor de securitate cibernetică.

IDENTIFICARE

Angajatul a anunțat imediat furtul poliției și companiei sale. De asemenea, banca a fost informată să monitorizeze tranzacțiile din cont. Compania a informat în consecință compania care sprijină TIC să dezactiveze accesul de la distanță al laptopului și a început activitatea de monitorizare. Laptopul era echipat cu instrumente de securitate și protecție prin parolă. Datele stocate pe hard disk nu au fost criptate - acestea includ date sensibile ale clienților și detalii bancare ale companiei.

Pentru o identificare bazată pe comportament a acestui atac, pot fi utilizate următoarele tehnici MITRE ATT&CK:

- ☑ T1027 - Fișiere sau informații ascunse
- ☑ T1036 Mascarada
- ☑ T1586.002 – Conturi compromise: Conturi de e-mail

RĂSPUNS

Răspuns: Compania trebuie să respecte legile de stat în ceea ce privește o încălcare a datelor. Legile de stat și reglementările UE privind GPDR sunt foarte stricte, cu amenzi mari.

- ☑ **CINE:** Atacatorul nu a putut fi identificat. Se știa doar locul incidentului.
- ☑ **PE CINE:** Fără țintă specifică

- ☑ **DE CE:** Colectarea de date sensibile și câștigarea de bani din vânzarea echipamentului furat.
- ☑ **CE:** Datele sensibile ale clienților și detaliile bancare ale companiei.
- ☑ **CUM:** Pierderi de echipamente, scurgeri de date sensibile și atac de cont bancar.
- ☑ **STRATEGIA:** Amenințarea a început pe un computer fără antivirus și s-a răspândit lateral. O firmă specializată TIC a efectuat un proces de curățare.

RECUPERARE

IMPACT: Compania de consultanță a cheltuit peste 20.000 de euro pentru implementare, monitorizare și îmbunătățiri operaționale. O încălcare a datelor are un impact negativ asupra unei mărci și încrederea trebuie reconstruită.

Principalele consecințe ale atacului au fost următoarele:

- ☑ Pierderea datelor
- ☑ Pierdere PC
- ☑ Sistem compromis
- ☑ Costuri financiare

RECUPERARE: Strategia de recuperare a fost concentrată pe minimizarea reputației mărcii și pe monitorizarea și controlul sistemelor interne și a conturilor bancare ale companiei. Preventiv, toate acreditările contului bancar s-au schimbat, iar privilegiile sistemelor angajaților au fost suspendate și modificate.

STRATEGIA: Compania ar trebui să implementeze diverse acțiuni pentru a preveni astfel de incidente. Strategia sa trebuie să se concentreze asupra:

- ☑ Efectuării de programe de instruire pentru a asigura gradul de conștientizare a angajaților
- ☑ Efectuarea de controale și audituri regulate
- ☑ Să efectueze prevenirea şi implementarea unui sistem de management al riscurilor.

LECȚII ÎNVĂȚATE

- ☑ Companiile trebuie să stabilească și să instruiască angajații cu privire la manipularea în siguranță a dispozitivelor eliberate de serviciu.
- ☑ Dispozitivele trebuie depozitate în siguranță atunci când nu sunt în prezența imediată a angajatului.
- ☑ Companiile trebuie să ia măsuri pentru a cripta datele oriunde sunt stocate sau transmise.

- ☑ Angajații trebuie să aibă o înțelegere clară a importanței criptării și a modului de utilizare.
- ☑ Companiile trebuie să înțeleagă și să cunoască responsabilitățile care le revin conform legilor privind notificarea încălcării datelor din țara în care își desfășoară activitatea.
- ☑ O revizuire regulată a practicilor de securitate ale companiei este imperativă în organizațiile moderne pentru a preveni incidentele, a descoperi vulnerabilități și a reduce impactul incidentelor.

STUDIU DE CAZ 18: ATACUL DDOS OPREȘTE SERVICIILE IMPORTANTE

ORGANIZAȚIA ȚINTĂ

Organizația vizată a fost o companie de găzduire. Atacatorii au lansat un atac masiv distribuit de refuzare a serviciului împotriva unui anumit site web la mijlocul lui decembrie 2021, depășind o lățime de bandă de 1,5 gigabiți pe secundă și aproape 100 de milioane de pachete pe secundă, cel mai mare atac cu care se confruntă o companie de găzduire.

Compania crede că atacatorul s-a concentrat pe site-urile web cu jocuri de cazino online, iar furnizorul de găzduire nu a fost ținta reală. Atacul DDOS determină întreruperea disponibilității serviciilor clientului pentru mai mult de 12 ore.

Un atac de refuzare a serviciului distribuit (DDoS) este o încercare rău intenționată de a perturba traficul normal al unui server, serviciu sau rețea vizat prin copleșirea țintei sau a infrastructurii înconjurătoare cu un flux de trafic pe Internet. Atacurile DDoS obțin eficacitate prin utilizarea mai multor sisteme informatice compromise ca surse de trafic de atac. Mașinile exploatate pot include computere și alte resurse în rețea, cum ar fi dispozitivele IoT.

"A existat o creștere cu 57% a variantelor de botnet Mirai identificate în 2019. Variantele Mirai sunt de obicei utilizate pentru atacuri cu forță brută pe dispozitivele IoT. Aceste atacuri au crescut cu 51%, în timp ce exploit-urile web au crescut cu 87% în 2019." (MCCART, 2022).

CUM S-A OBȚINUT INFORMAȚIA?

Informațiile necesare pentru a descrie acest atac cibernetic au fost colectate prin două interviuri (întâlniri față în față), unul cu CEO-ul companiei și unul cu un inginer TI al companiei. Ambii au fost dispuși să descrie și să dea detalii despre incident, dar au cerut să păstreze anonimatul ambelor companii și numele lor, deoarece informațiile erau prea sensibile pentru ei.

PREVENIRE

Deși furnizorul de găzduire are mai multe proceduri și mecanisme de securitate cibernetică, se pare că atacatorii au găsit un punct vulnerabil de explorat.

Tehnicianul companiei a observat că site-ul web a devenit brusc lent, dar presupun că a fost o creștere legitimă a traficului din cauza sezonului sărbătorilor. Atacul a fost identificat imediat după ce site-ul a devenit indisponibil și clientul s-a plâns.

IDENTIFICARE

Atacatorii au folosit trafic din surse din întreaga lume. Se pare că atacul de denial-of-service a fost creat de un botnet Mirai. Și pentru că botnet-ul Mirai are capacitatea de a trimite aproximativ 600 de megabiți pe secundă, au folosit un atac de nivel al doilea cu un alt botnet Mirai.

Mirai este un malware care infectează dispozitivele inteligente care rulează pe procesoare ARC, transformându-le într-o rețea de roboți controlați de la distanță sau „zombi". Această rețea de roboți, numită botnet, este adesea folosită pentru a lansa atacuri DDoS.

Furnizorul de găzduire a folosit instrumente de analiză a traficului pentru a identifica atacul. Caracteristica de bază a atacului este volumul mare care provine din aceeași serie de adrese IP. Inginerii reușesc să izoleze acele IP-uri și site-ul a revenit.
După aceea, încearcă să identifice de ce instrumentul de analiză a traficului nu a detectat atacul încă din primele etape.

Conform cadrului MITRE ATT&CK, această incidență poate fi descrisă după cum urmează:

- ☑ T1499 - Refuzarea serviciului de la punctul final
- ☑ T1498 - Refuzarea serviciului în rețea

RĂSPUNS

- ☑ **CINE:** Atacatorul nu poate fi identificat. Atacul a venit din toată lumea.
- ☑ **PE CINE:** Ținta a fost un site web specific care găzduiește jocuri de cazinou online.
- ☑ **DE CE:** Pentru a-i întrerupe funcționarea.
- ☑ **CE:** Site-ul companiei.
- ☑ **CUM:** Atacul DDOS folosind botnet-urile Mirai.
- ☑ **STRATEGIA:** Atacul a început asupra unui server de furnizor de găzduire pentru a întrerupe funcționarea unui anumit site web. Instrumentul de analiză a traficului nu a reușit să alerteze pentru posibilitatea unui atac cibernetic. Compania a crescut sensibilitatea alarmelor din instrumentul de analiză a traficului, astfel încât să evite incidente similare pe viitor.

RECUPERARE

IMPACT: Furnizorul de găzduire a avut niște costuri suplimentare semnificative pentru a acoperi atacul și, de asemenea, a avut daune grave reputației. Au avut costul suplimentar cu forța de muncă pentru a recupera site-ul web și penalitățile privind acordul SLA cu clientul. Costul total a fost estimat la aproximativ 40.000 de euro.

RECUPERARE: Strategia de recuperare a fost axată pe izolarea IP-urilor atacatoare pentru a opri atacul și a recupera funcționarea site-ului web. Alte acțiuni au fost creșterea sensibilității alarmelor a instrumentului de analiză a traficului. S-au verificat toate serverele și serviciile de găzduire pentru orice alte atacuri sau activități suspecte.

STRATEGIA: Compania ar trebui să implementeze diverse acțiuni pentru a preveni astfel de incidente. Strategia sa trebuie să se concentreze asupra:

- ☑ Creșterea sensibilității instrumentului de analiză a traficului
- ☑ Instalarea unui al doilea instrument pentru securitate suplimentară
- ☑ Efectuarea de programe de instruire pentru a asigura gradul de conștientizare a angajaților
- ☑ Restricționarea unor intervale de IP
- ☑ Efectuarea de controale și audituri regulate
- ☑ Să efectueze prevenirea şi implementarea unui sistem de management al riscurilor
- ☑ Să își certifice infrastructura și serviciile conform ISO 27001 și ISO 22301.

LECȚII ÎNVĂȚATE

- ☑ Perturbarea vine sub mai multe forme. Întreruperile sau întârzierile pot apărea sub mai multe forme, în special pentru furnizorii de găzduire. Atunci când un atac este identificat, echipe de răspuns adecvate trebuie să dedice resurse pentru a face față acestuia.
- ☑ Multe atacuri cibernetice sunt ușor de prevenit. Atacurile cibernetice sofisticate pot provoca multe daune, dar multe dintre ele pot fi prevenite cu ușurință cu securitatea adecvată. Este important să construiți un sistem de management al securității puternic și proactiv pentru a opri atacurile. Un astfel de sistem de management necesită întreținere continuă, monitorizarea tuturor sistemelor și dispozitivelor din rețea, inclusiv actualizarea tehnologiei și aplicarea de corecții de securitate pentru exploit-urile cunoscute.
- ☑ Atacurile DDoS trebuie luate în serios. Atacurile DoS și DDoS de astăzi sunt diferite, deoarece sunt mai vicioase, mai ascuțite și mai capabile.
- ☑ Limită de timp. Atacurile la nivelul rețelei pot dura mai mult de 48 de ore, în timp ce atacurile la nivelul aplicației pot dura zile. Infiltrarea sistemelor și rețelelor pentru spionaj – săptămâni și luni.
- ☑ Securitatea cibernetică ar trebui să fie o prioritate. Securitatea cibernetică ar trebui să fie una dintre cele mai înalte priorități pentru toate entitățile care operează în peisajul actual. Aceste atacuri au devenit sofisticate, direcționate, capabile și nereglementate. Toate amenințările ar trebui luate în serios, inclusiv atacurile DDoS, care sunt din ce în ce mai frecvente.

CONCLUZII

Pe baza portofoliului diversificat care este prezentat în cadrul bateriei documentare ENCRYPT 4.0 privind atacurile cibernetice, se pot trage următoarele concluzii:

- ☑ Odată cu dezvoltarea TIC și în contextul Industriei 4.0, securitatea cibernetică are o importanță tot mai mare, iar **companiile care nu au o apărare cibernetică adecvată își pun operațiunile în pericol grav.**
- ☑ **Angajații joacă un rol cheie în apărarea cibernetică,** prin urmare, atât angajații din cadrul IMM-urilor, cât și al marilor întreprinderi ar trebui să primească cel puțin o formare de bază despre cum să protejeze datele companiei și să lucreze cu informații sensibile, deoarece mai multe atacuri cibernetice au loc din cauza lipsei de cunoștințe privind aceste aspecte, mai ales în contextul lucrului la distanță în timpul pandemiei de COVID-19.
- ☑ **IMM-urile, care nu țin cont de sectorul în care își desfășoară activitatea, devin ținte principale pentru hackeri și infractorii cibernetici organizați,** dar, în același timp, doar 1/3 dintre IMM-uri au un plan pentru a limita un potențial atac cibernetic și prin urmare IMM-urile trebuie să prevadă securitatea cibernetică în topul priorităților pentru a le asigura competitivitatea pe termen lung.

BIBLIOGRAFIE

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

2. Barber, B., 2016. William Hill apologise after website attack. [Online] Racing Post. Available at: https://www.racingpost.com/news/william-hill-apologise-after-website-attack/266196 (Studiu de caz 6)

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

4. Braue, D., 2022. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. [Online] 2022 Cybersecurity Ventures. Available at: 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. Available at:https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

6. Craver, R., 2015. Hanesbrands database hacked900K phone, online customers affected. [e-journal] *Winston-Salem Journal.* Available at: https://journalnow.com/business/hanesbrands-database-hacked/article_543b338e-3664-11e5-b77e-c77df1e08b5c.html (Studiu de caz 4)

7. Cyber Startup Observatory. Available at: https://cyberstartupobservatory.com/ (Case study 4)

8. CyberNews, 2021. Thousands of Humana customers have their medical data leaked online by threat actors. [Online] 2022 Cybernews. Available at: https://cybernews.com/news/humana-insurance-customers-medical-data-leaked/(Studiu de caz 5)

9. CyberTalks, 2022. Top 15 phishing attack statistics (and they might scare you) [Online]. CyberTalks. Available at: 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. Available at: https://cyware.com/news/humana-websites-hit-by-sophisticated-spoofing-attack-from-foreign-countries-5ac77624 (Studiu de caz 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. Available at: https://www.databreaches.net/humana-notifies-members-after-credential-stuffing-attack-on-humana-com-and-go365-com/ (Studiu de caz 5)

12. EUROPOL, n.d. World's most dangerous malware EMOTET disrupted through global action. [Online] EUROPOL 2022. Available at: 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*. Available at: https://www.databreachtoday.asia/humana-notifying-victims-identity-spoofing-attack-a-11153(Studiu de caz 5)

14. McCart, C., 2022. 15+ Shocking botnet statistics. [Online] Comparitech. Available at: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. Available at: 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. Available at: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

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

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

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

20. VentureBeat, 2022. Report: Average time to detect and contain a breach is 287 days. [Online] VentureBeat. Available at: 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. Available at: 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.Available at: https://lab.wallarm.com/the-biggest-hacker-attacks-on-gambling/ (Studiu de caz 6)

ENCRYPT 4.0

Cofinanțat prin programul Erasmus+ al Uniunii Europene

PARTENERI DE PROIECT

ENCRYPT 4.0

Inițiativa comună de dezvoltare a forței de muncă cibernetice pentru a permite industriei europene să depășească deficitul de profesioniști în securitate cibernetică

Proiectul ENCRYPT4.0 (2020-1-RO01-KA202-079983) își propune să faciliteze managementului IMM-urilor din producție să adopte o abordare proactivă față de securitatea cibernetică prin sprijinirea acestora în procesul de analiză, identificare și abordare a riscurilor și amenințărilor cibernetice aplicabile organizației lor prin promovarea învățării interactive bazate pe proiecte în ceea ce privește stimularea abilităților și competențelor în domeniul securității cibernetice ale angajaților IMM-urilor sau/și ale profesioniștilor din domeniul securității cibernetice.

Universitatea de Medicină, Farmacie, Științe și Tehnologie „George Emil Palade” din Târgu Mureș - România

Coordonator de proiect

European Center for Quality Ltd., Companie de consultanță - Bulgaria

Instituto de Soldadura e Qualidade, Instituție tehnologică - Portugalia

Avantalia, IMM bazat pe tehnologie - Spania

FH Joanneum, Universitatea de Științe Aplicate - Austria

PCX Management, Computers & Information Systems Ltd. - Cipru