ENCRYPT 4.0

Apoiar a Indústria Europeia Através da Capacitação de Profissionais de Cibersegurança

Nº 2020-1-RO01-KA202-079983

O3: Repositório sobre ciberataques

Cofinanciado pelo Programa Erasmus+ da União Europeia

Projecto financiado com o apoio da Comissão Europeia. A informação contida nesta publicação vincula exclusivamente o autor, não sendo a Comissão responsável pela utilização que dela possa ser feita.

CONTEÚDOS

INTRODUÇÃO

Com o aparecimento das TI e na ascensão da quarta revolução industrial, as empresas enfrentam novos desafios ligados à cibersegurança e à proteção de dados. Isto é especialmente válido para as PME de fabrico que muitas vezes não têm os recursos internos e a capacidade de avaliar eficazmente os riscos de cibersegurança correspondentes às tecnologias recém-implementadas da Indústria 4.0. Ao mesmo tempo, as PME estão a tornar-se com mais frequência vítimas de cibercrimes. De acordo com o Relatório de Investigações de Violação de Dados *da Verizon 2021 (Verizon, 2021)*, as PME são vítimas e são mais vulneráveis a ciberataques do que as grandes empresas, uma vez que carecem de recursos, pessoas, informação e capacidade geral para evitar os riscos de um ciberataque.

As ciberameaças vêm de fontes variadas e estão a tornar-se mais sofisticadas, ex: se as equipas não experimentaram vulnerabilidades semelhantes e não tiverem uma orientação clara sobre como responder, pode levar dias e até semanas a reagir corretamente, o que pode ser fatal para alguns processos de fabrico. De acordo com o Relatório de Segurança da SMB 2021, os funcionários que não seguem as orientações são considerados como a principal barreira à cibersegurança e esta tendência agravou-se com o aumento do trabalho remoto devido à pandemia COVID-19 *(Untangle, 2021).* No entanto, quando há uma violação da cibersegurança, não afeta apenas as pessoas, pode muito bem causar perdas financeiras, a confiança dos clientes e a reputação danificada *(Acronis, 2021).*

O consórcio do projeto Encrypt 4.0 desenvolveu este documento para servir como uma ferramenta de saber-fazer que dá acesso a análises críticas de verdadeiros ciberataques e as lições aprendidas, assim como o roteiro sobre como prevenir, identificar, atacar e recuperar destes ataques.

O repositório de informação Encrypt 4.0 sobre ciberataques é adaptado às necessidades das PME de fabrico que operam no contexto da Indústria 4.0 e representa uma compilação de casos de estudos, com o objetivo de apoiar as PME no reforço da sua cibersegurança e na prevenção de ciberataques.

ESTRUTURA & METODOLOGIA

Apresentamos aqui um total de **18 estudos de caso**. Cada um dos parceiros do projeto desenvolveu 3 estudos de caso sobre ciberataques com base em pesquisas, experiência pessoal, observação e entrevistas a gestores de empresas, profissionais de cibersegurança e especialistas em TI que cobrem vários tipos de ciberataques e dão uma análise crítica das razões das falhas de segurança, como foram abordadas e quais foram as suas consequências.

O consórcio ENCRYPT 4.0 construiu um modelo específico "PREVENIR-IDENTIFICAR-RESPONDER-RECUPERAR" (PIRR) baseado no modelo "Identificar, Proteger, Detetar, Responder e Recuperar" do Instituto Nacional de Normalização e Tecnologia (NIST). O tipo de ciberataques baseia-se no modelo STRIDE[1], e no quadro MITRE ATT&CK. A análise do modelo PIRR contém 4 categorias principais baseadas nos passos principais para combater um problema de segurança cibernética, bem como as secções aprendidas (ver Fig. 1.).

Fig. 1. Categorias do modelo (PIRR) "Prevenir – Identificar – Responder – Recuperar"

[1] Pode ler mais sobre o modelo STRIDE aqui:

- Benjamin, P., 2018. Desmistificar modelos de ameaça STRIDE [online]. Comunidade DEV. Disponível em: https://dev.to/pbnj/demystifying-stride-threat-models-230m;

PREVENIR

Esta secção centra-se na redução do risco de exposição a ciberataques e medidas preventivas e para cada estudo de caso inclui o seguinte:

- Práticas de segurança específicas estabelecidas que tiveram efeitos comprovados em verdadeiros ciberataques;
- Equívocos de segurança cibernética: práticas que cada empresa aplicou e teve impacto zero ou mesmo negativo em incidentes reais.

IDENTIFICAR

O principal objetivo desta secção é ajudar as PME a distinguir entre os diferentes tipos de ciberataques categorizados utilizando o modelo STRIDE e os quadros ATT&CK do MITRE. O modelo STRIDE representa um modelo de ameaça de alto nível centrado no sistema focado na identificação de categorias globais de ataques. Tem as seguintes 6 categorias:

+Adulteração

+Repúdio

+Divulgação de informação

+Negação de serviço

+Elevação do privilégio

Para os estudos de caso ENCRYPT 4.0, o STRIDE foi utilizado para identificar as ameaças a um nível mais elevado, enquanto o quadro MITRE ATT&CK foi aplicado para especificar os ataques com mais pormenor. O quadro ATT&CK toma intencionalmente o ponto de vista de um atacante para ajudar as organizações a entender como os adversários se aproximam, se preparam e executam com sucesso ataques.

RESPONDER

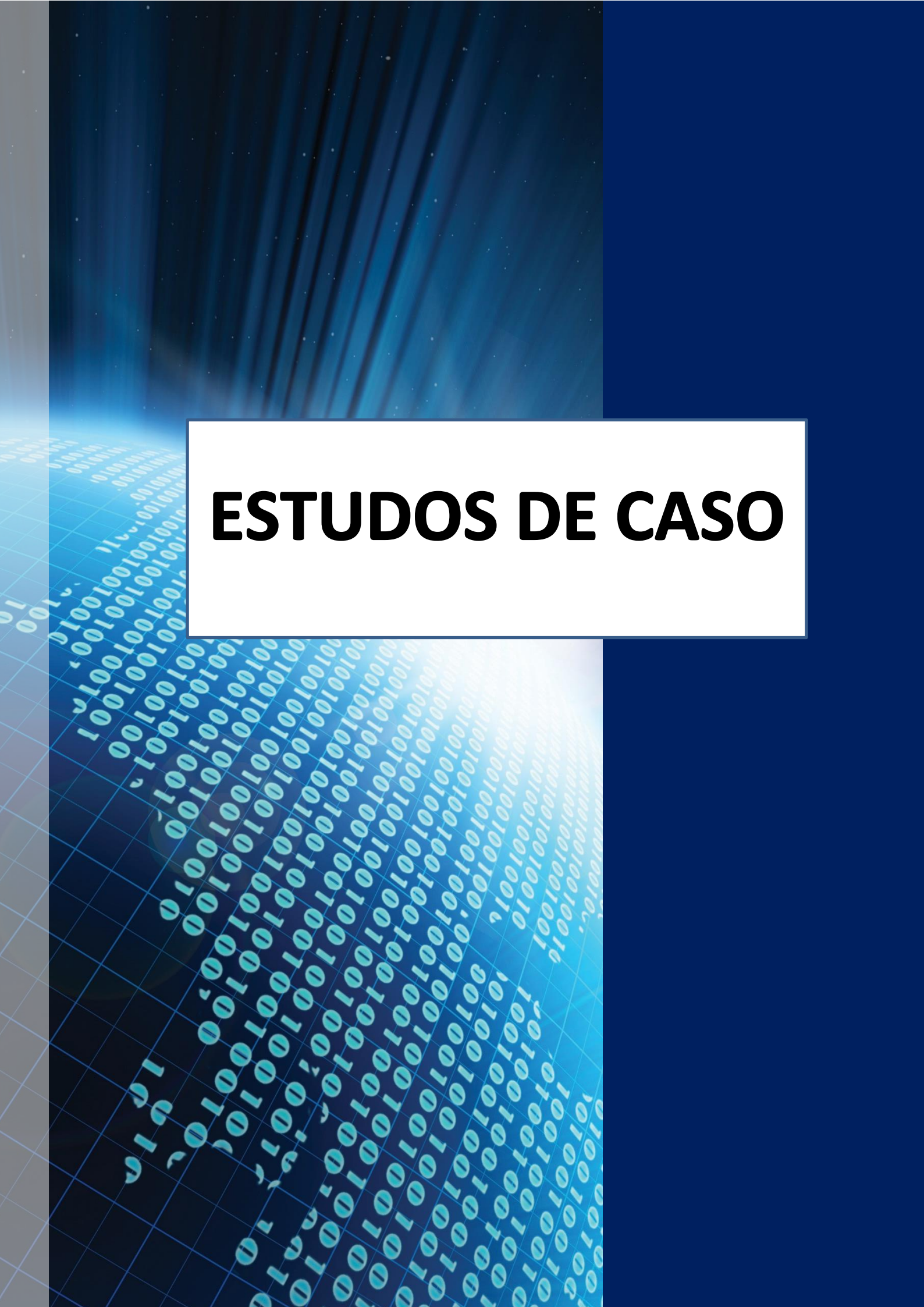
Esta secção retrata as situações em que a ameaça já está presente, fornecendo análises de verdadeiros ciberataques e conselhos sobre como reagir em casos semelhantes após identificá-los.

Os ciberataques dentro dos estudos de caso são delineados no seguinte formato:

- QUEM: o atacante
- A QUEM: a organização-alvo
- PORQUÊ: os motivos por detrás do ataque (foi aleatório ou visado)
- O QUE: a propriedade alvo
- COMO: descrição do ataque e quais foram as técnicas utilizadas.
- ESTRATÉGIA: como foi abordada a ameaça e as medidas que tiveram efeito zero ou negativo.

RECUPERAR

A secção fornece informações sobre quais foram as consequências do ataque, bem como análises sobre como realizar uma recuperação do sistema depois de alguns processos terem sido danificados e recuperar o acesso aos dados que foram perdidos, com base nos casos reais de ataque descritos na secção RESPONDER. A secção segue os modelos STRIDE & MITRE ATT&CK que delineam práticas de recuperação com base em cada grupo especificado de ameaças cibernéticas apresentadas na secção IDENTIFICAR.


ESTUDOS DE CASO

ESTUDO DE CASO 1: A APARÊNCIA INVERSA

A ORGANIZAÇÃO-ALVO

A Associação Innovalia é um centro tecnológico privado e independente que foi criado pelo Grupo Innovalia para articular uma massa crítica capaz de alcançar com sucesso as suas ambições de investigação a longo prazo e objetivos estratégicos. Innovalia é uma aliança para PME na área da tecnologia com sede em Espanha. Tem uma presença internacional com escritórios no País Basco, Madrid, Catalunha, Ilhas Canárias, Europa, Ásia, Médio Oriente e América Central e do Sul. Desde a sua fundação, a Associação Innovalia desenvolveu uma sensibilidade especial e apoio na consciencializaçãoação para as características específicas das PME com base na tecnologia. Hoje, tornou-se um líder na área de I&D por e para as PME em Espanha. Oferece também soluções para facilitar os processos internacionais de inovação dirigidos às PME. Como agente tecnológico da Rede de Tecnologia do País Basco (Innobasco), a Innovalia reúne as competências, laboratórios e recursos das empresas que fundaram a associação.

COMO FOI RECOLHIDA A INFORMAÇÃO?

A informação para este estudo de caso foi recolhida através de uma entrevista aprofundada com o técnico de TI da empresa. Durante a interação, o entrevistador colocou perguntas iniciais, às quais o entrevistado foi encorajado a responder. A informação em falta foi *completada à posteriori* com a informação dada pela pessoa entrevistada.

PREVENIR

A prática que a Innovalia aplicou antes do incidente foi a instalação de um software de **firewall**.

Práticas de segurança específicas:

- ☑ **a consciência dos funcionários sobre e-mails não fidedignos.** Neste caso, um hacker enviou um e-mail aparentemente legítimo a pedir aos colaboradores que clicassem num link para redefinir a senha de acesso, a pretexto de que tinham sido registadas várias tentativas de login mal sucedidas.
- ☑ **a instalação de firewall internas** para reforçar a sua firewall externa padrão. Quando o pessoal trabalhava a partir de casa durante a pandemia COVID-19, eram obrigados a instalar uma firewall na sua rede doméstica.

"A injeção de comando é um ciberataque em que um intruso assume o controlo do sistema operativo do host em código numa aplicação vulnerável através de um comando. Este código é executado apesar de qualquer mecanismo de segurança e pode ser usado para roubar dados, sistemas de falhas, bases de dados de danos e até mesmo instalar malware que pode ser usado mais tarde". (StackHawn, 2022)

IDENTIFICAR

O tipo e a natureza do ciberataque foi: **Injeção de código numa vulnerabilidade no servidor web apache da empresa através da execução remota de comando**. Este tipo de ataque pode ser descrito em detalhe de acordo com o quadro ATT&CK do MITRE, como mostrado abaixo.

- ☑ Reconhecimento: Digitalização ativa: Digitalização de blocos IP e digitalização de vulnerabilidades
- ☑ Acesso Inicial: Serviços Remotos Externos
- ☑ Execução: Intérprete de Comando e Script: Power Shell
- ☑ Escalada de Privilégio:
  - Injeção de processo: Injeção de biblioteca de ligação dinamica; Injeção executável portátil; Sequestro de execução de fios; Chamada de Procedimento Assíncrona; Thread de Armazenamento Local; Chamadas do Sistema Ptrace; Memória Proc; Injeção extra de memória da janela;
  - Execução desencadeada por evento: Modificação da configuração da camada unix,
- ☑ Evasão da defesa: Injeção de processo e modelo
- ☑ Exfiltração: Transferir dados para a Conta Cloud
- ☑ Impacto:
  - Manipulação de dados: Manipulação de dados armazenados, transmitidos e em tempo de execução
  - Paragem de Serviço
  - Sistema Desligar/Reiniciar

RESPONDER

- ☑ **QUEM:** O agressor foi identificado, só o local de origem, a China.
- ☑ **A QUEM:** Associação Innovalia
- ☑ **PORQUÊ:** Aleatório
- ☑ **O QUE:** Sistema da organização Innovalia
- ☑ **COMO:** Injeção de processo com execução de comando remoto.
- ☑ **ESTRATÉGIA:** A ameaça foi abordada com a firewall que o servidor tinha naquele momento. Siga os passos descritos na secção seguinte, sobre como bloquear os IP.

RECUPERAR

As principais consequências do ataque foram:

- ☑ Sistema comprometido
- ☑ Investigação e Análise
- ☑ Atualização da versão do servidor

☑ Alterar credenciais

A **estratégia de recuperação** focou-se em bloquear o IP através da firewall:

Em primeiro lugar, inicie sessão no servidor no qual necessita de bloquear o endereço IP. Em seguida, clique em Iniciar, digite Firewall com segurança avançada e prima Enter. No painel esquerdo, clique em Regras de Entrada para mostrar as regras atualmente configuradas no painel central.

No painel direito, clique em Ações > Nova Regra: Para Tipo de Regra, selecione Personalizado e clique em Seguinte; para Programar, selecione Todos os programas e clique em Seguinte; para Protocolo e Portas, selecione Qualquer a partir do dropdown do tipo de protocolo e clique em Seguinte; e para Scope: em que endereços IP remotos esta regra se aplica?, selecione a opção radial: Estes endereços IP: Clique em Adicionar.

Em seguida, insira o endereço IP que pretende bloquear a partir do servidor e clique em OK. Também pode optar por bloquear uma série de endereços IP selecionando a gama de endereços IP: opção radial. Depois de terminar de adicionar os endereços IP, clique em Seguinte. Para Ação, selecione Bloquear a ligação e clique em Seguinte. Para Perfil, deixe todas as opções verificadas e clique em Seguinte. Para nome, dê à regra um nome descritivo, como IPs blacklist. Também pode introduzir uma descrição opcional da regra. Clique em Terminar. A regra recém-criada com o nome próprio agora aparece no painel de regras de entrada média. Para ordenar as regras alfabeticamente pelo nome, pode clicar no cabeçalho da coluna Nome. Se precisar de desativar a regra, clique com o botão direito na regra da lista e clique em 'Regra de Desativar'. Se precisar de modificar o âmbito de aplicação dos endereços IP para a regra, clique com o botão direito na regra da lista e clique em Propriedades. Em seguida, clique no separador Âmbito, faça as alterações necessárias e clique em Aplicar.

LIÇÕES APRENDIDAS

Aprendemos que é melhor ter certas medidas preventivas e defensivas, que são úteis para este tipo de ataques, tais como:

- ☑ Para manter o servidor atualizado
- ☑ Para adicionar monitorização à máquina do servidor
- ☑ Para segmentar a rede em VLANS, e
- ☑ Isolar máquinas expostas ao exterior.

ESTUDO DE CASO 2: O DESCUIDO DE UM EMPREGADO

PREVENIR

A organização aplicou o Sistema de Deteção de Intrusões (IDS), que monitoriza a rede CARSA para atividades maliciosas ou violações de políticas. A CARSA aplica software de firewall para proteger a sua rede e sistema de acesso não autorizado.

Práticas de segurança específicas estabelecidas que tiveram efeitos comprovados noutros ciberataques são:

"Em 2021, 83% das organizações relataram ter sofrido ataques de phishing. Em 2022, espera-se que ocorram mais seis mil milhões de ataques." (CyberTalk, 2022)

Validar e limpar entradas: Procure caracteres de escape e outros símbolos especiais para o idioma de aplicação e sistema operativo, tais como marcas de comentários, caracteres de terminação de linha e delimitadores de comando. Se a aplicação espera apenas um conjunto limitado de valores, aceite apenas esses valores, por exemplo, por whitelisting ou ligando-os condicionalmente.

Evite construções de avaliação vulneráveis: evitamos a utilização de funções "eval()" e equivalentes nas entradas de utilizadores brutos. A CARSA utilizou funcionalidades específicas da linguagem dedicadas para processar com segurança os argumentos fornecidos pelo utilizador.

Bloqueie o intérprete: Se tiver controlo sobre a configuração do servidor, é melhor limitar a funcionalidade do intérprete ao mínimo necessário para a aplicação para evitar uma escalada na injeção de comando do sistema. Por exemplo, se a sua aplicação PHP não utilizar a função do sistema() pode desativar essa função no seu ficheiro php.ini especificando-a na diretiva disable_functions. As funções geralmente desativadas para PHP incluem: exec(), passthru(), shell_exec(), sistema(), proc_open(), popen(), curl_exec(), curl_multi_exec(), parse_ini_file() e show_source().

Consulte o nosso código: A CARSA utilizou ferramentas de verificação de código estático para procurar vulnerabilidades relacionadas com a validação de entradas e avaliação insegura.

Digitalize as aplicações: a organização utilizou um scanner para garantir que as aplicações estão seguras de vários tipos de ataques. Por exemplo, a CARSA tem um Sistema de Deteção de Intrusões.

IDENTIFICAR

O ciberataque ocorreu dentro da CARSA, e o tipo de cyber-attack foi um **"ataque de phishing**". O ataque de phishing um tipo de ataque de engenharia social frequentemente usado para roubar dados de utilizadores, incluindo credenciais de login.

De acordo com o modelo STRIDE, este tipo de ataque tem como "Ameaça" a elevação do privilégio, porque o imóvel violado é a "autorização". Neste tipo de ciberataque, o utilizador permite que alguém faça algo que não está autorizado a fazer.

De acordo com o quadro MITRE ATT&CK, este ataque é:

☑ Reconhecimento: Phishing para informações: Serviço de spearphishing, acessório de spearphishing e link de spearphishing.

☑ Acesso inicial: Phishing: Anexos de spearphishing, ligação ou via Serviço.

☑ Execução: Os adversários podem enviar mensagens de phishing para ter acesso aos sistemas de vítimas. Todas as formas de phishing são

eletronicamente entregues através de engenharia social. O Phishing pode ter um alvo, conhecido como spearphishing. No spearphishing, um indivíduo específico, empresa ou indústria será alvo do adversário. De uma forma mais geral, os adversários podem realizar phishing não direcionado, como em campanhas de spam de malware em massa.

☑ Discovery: a deteção poderia ser feita através de: Registo de aplicações (conteúdo), ficheiro (criação de ficheiros) ou o tráfego da rede (conteúdo ou fluxo)

☑ Movimento Lateral: Spearphishing interno

☑ Exfiltração: Engenharia Social e Ataques de Phishing; correio de saída, downloads para dispositivos inseguros, uploads para serviços externos e comportamento inseguro na nuvem

☑ Impacto: perda de dados sensíveis, danos de reputação, cliente ou cliente, custo de tempo de inatividade, etc.

RESPONDER

QUEM: O agressor era uma pessoa/organização externa desconhecida, através de um funcionário da CARSA.
A QUEM: As credenciais de acesso a um software de pagamento (sem público ou open-source).
PORQUÊ: O roubo de credenciais, bem como informações confidenciais da entidade.
O QUÊ: Dados e senhas
COMO: Um funcionário instalou software que não era permitido pela empresa como definido na política da empresa. Este tipo de software não era permitido devido à fiabilidade e segurança duvidosas. (Geralmente, todo o software instalado nos computadores dos colaboradores deve ser supervisionado pelo pessoal técnico informático da entidade.) Este software tinha um “cavalo de troia” na rede. Há várias maneiras pelas quais um “Trojan” ataca um sistema, neste caso particular, foi um "cavalo de troia infostealer", como parece, este “Trojan” está atrás de dados no computador infetado.
ESTRATÉGIA: A estratégia seguida foi rastrear o endereço Mac para identificar a máquina infetada e o funcionário responsável. Mais tarde, o software foi removido, assim como o vírus.

RECUPERAR

IMPACTO: roubo de credenciais de utilizador a nível local

ESTRATÉGIA DE RECUPERAÇÃO:

☑ Através do endereço Mac sabíamos que funcionário estava a ser atacado, sem que ele se apercebesse.

☑ O software que não deveria ter sido instalado foi desinstalado

- ☑ Um antivírus e programas antimalware foram executados na máquina específica.
- ☑ Alterar credenciais de utilizador comprometidas

MELHOR ESTRATÉGIA: o computador tem de ser formatado porque nunca se pode ter a certeza da sua eliminação completa.

LIÇÕES APRENDIDAS

Aumentar a responsabilidade dos colaboradores através de:

- ☑ formação com palestras curtas sobre a importância de não instalar software e confirmação de segurança não anunciados da equipa de suporte técnico e,
- ☑ lembrando as políticas de segurança da empresa e os regulamentos comuns de segurança em cibersegurança.
- ☑ Para atualizar o software das máquinas da empresa (software: janelas e programas antivírus). Para lembrar os empregados para executar o exame antivírus várias vezes.

ESTUDO DE CASO 3: O CARTÃO DE CRÉDITO DE UMA PME VIA REDE WIFI

A ORGANIZAÇÃO-ALVO

Bodegas Monje está localizado num enclave excecional da ilha de Tenerife, no local conhecido como "La Hollera" no município de El Sauzal com vista para o Teide. Uma longa tradição de produtores de vinho acompanha a família Monje desde 1750. Barris de carvalho e modernos sistemas de maceração coexistem para dar aos vinhos tintos, brancos e rosés um caráter e sabores especiais, que estão perfeitamente adaptados à melhor gastronomia das Ilhas Canárias. Esta adega acolhe ainda iniciativas culturais, gastronómicas e de lazer que expandem as fronteiras do vinho e a devolvem ao ambiente social de onde historicamente vem, um verdadeiro compromisso com o enoturismo: Wine&Tours.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

O método aplicado para recolher a informação para este estudo de caso foi a entrevista.

PREVENIR

A organização não aplicou nenhuma prática de cibersegurança antes deste evento. Só têm uma firewall no Fornecedor de Serviços de Internet (Router Movistar).

As práticas específicas de segurança estabelecidas em Bodegas Monje que tiveram efeitos comprovados na prevenção deste tipo de incidente foram agendadas após o evento. Em particular, as ações tomadas foram bem sucedidas na prevenção de novos ataques de natureza semelhante.

IDENTIFICAR

Um cliente do estabelecimento acedeu à empresa para consumir os produtos produzidos, e ligou-se à internet através da rede WIFI. O ciberataque foi identificado pelo próprio cliente afetado. Esta pessoa detetou movimentos nas suas contas bancárias com pagamentos online feitos com o seu cartão de crédito, mas não por ele. Todos estes movimentos foram feitos logo após a sua visita à empresa "Bodegas Monje".

O cliente alertou o banco para tentar cancelar esses pagamentos e bloquear o cartão para evitar que o cibercriminoso o continuasse a usar.

Posteriormente, notificou a empresa "Bodegas Monje", uma vez que foi o último local onde a usou.

RESPONDER

QUEM: um cliente da empresa que acedeu à rede local para fins ilegais.
A QUEM: a outro cliente, através da empresa**.**
PORQUÊ: para roubar dinheiro
O QUE: desviar os detalhes do banco e fazer encargos, beneficiando do dinheiro de outra pessoa
COMO: infiltração através da rede Wifi dos clientes
ESTRATÉGIA: Redesenhar a rede para separar a ligação dos clientes que visitam o negócio do sistema de pagamento e da rede interna da empresa.

RECUPERAR

IMPACTO:

☑ O cartão de crédito de um cliente comprometido

☑ A confiança dos clientes na segurança da empresa poderia ser comprometida e não serem capazes de confiar em fazer pagamentos por este método tão facilmente

☑ Se mais clientes fossem afetados por este ciberataque, isso teria um impacto direto na reputação da empresa.

ESTRATÉGIA DE RECUPERAÇÃO:

A estratégia levada a cabo pelo proprietário da empresa, a partir do momento em que tomou conhecimento do incidente, foi desligar o wi-fi e/ou desligar a rede de convidados. Depois, contactou uma empresa de cibersegurança para o resolver.

A nova estratégia de recuperação feita pela equipa de cibersegurança foi a de redesenhar a rede para separar a rede de clientes da rede interna da empresa, onde são armazenados os dados mais sensíveis (dados dos colaboradores e dos próprios clientes, como os dados do sistema de pagamento).

Nenhum dinheiro roubado poderá ser recuperado depois da rede ter sido redesenhada. O cliente teve que mudar o antigo cartão de crédito "roubado" por outro novo. A pessoa que realizou o ciberataque não foi identificada. Não foi possível tomar medidas legais.

Há uma estratégia melhor a ser levada a cabo nesta situação. Em vez de desligar a rede wi-fi da empresa, isto poderia ter sido feito além disso:

- ☑ Para fazer uma lista de todas as informações comprometidas, com todos os contactos de dados dos possíveis clientes que poderiam ser afetados (por linha temporal – de quem estava na empresa ao mesmo tempo que o cliente afetado).
- ☑ Informar outros clientes para estarem atentos a quaisquer movimentos estranhos nas suas contas bancárias efetuados com pagamentos online feitos com o seu cartão de crédito.
- ☑ Recolher o máximo de informação possível para não só ser capaz de identificar o culpado do ciberataque, mas também para alertar melhor os clientes que também podem ser afetados.
- ☑ Alterar imediatamente as palavras-passe para evitar o encerramento súbito da empresa, porque naquele momento, a rede não estava dividida, funcionou para os clientes e para os colaboradores ao mesmo tempo.

LIÇÕES APRENDIDAS

Entre as lições aprendidas, destacam-se as seguintes:

- ☑ que é melhor ter a rede segmentada
- ☑ que as políticas de confiança zero devem ser implementadas
- ☑ que não precisa ser uma grande empresa para sofrer um ciberataque

que é necessário dispor de equipamentos atualizados e sistemas de cibersegurança ativos (com firewall profissional, IPS, antivírus, etc.).

ESTUDO DE CASO 4: DIVULGAÇÃO DE INFORMAÇÃO HANESBRANDS INC.

ORGANISAÇÃO ALVO

A **Hanesbrands Inc.** (HBI) é uma empresa multinacional de vestuário fundada em 1901 e sediada em Winston-Salem, EUA. Têm mais de 250 pontos de venda em 47 países. Entre as marcas mais famosas

da empresa estão Hanes, Champion, Playtex, Bali, L'eggs, Just My Size, Barely There, Wonderbra, Duofold, Celebrity, Maidenform, Zorba, etc. Uma das vantagens competitivas da Hanesbrands é que 70% do vestuário que vendem é fabricado nas suas próprias instalações, bem como nos de empreiteiros parceiros. Desta forma, a empresa consegue controlar a maior parte da cadeia de fornecimento, o que também permite estabelecer práticas de sustentabilidade fortes e contribui para o seu sucesso mundial. Em 2021, a HBI foi nomeada uma das empresas mais éticas do mundo pela Ethisfera e tornou-se parte das 100 Empresas Mais Sustentáveis de Barron três anos num rolo. Para garantir que a empresa está a seguir uma política de sustentabilidade a longo prazo, estabeleceu metas globais de sustentabilidade para 2030 (em linha com os Objetivos de Desenvolvimento Sustentável das Nações Unidas sob três pilares: Pessoas, Planeta e Produto) e iniciou um website de sustentabilidade.

"De acordo com um novo relatório da Blumira e da IBM, o ciclo de vida de quebra média leva 287 dias, com como eventos a 212 dias a detetar inicial uma violação e 75 dias para conter a conter. " (VentureBeat, 2022)

Em 2019, a empresa teve receitas de 7 mil milhões de dólares e cerca de 61 mil colaboradores. Diz-se que a HBI está a gastar mais de $100.000 com cibersegurança, sobretudo em produtos Akamai, como serviços na nuvem.

COMO A INFORMAÇÃO FOI ADQUIRIDA?

O método aplicado para recolher as informações para este estudo de caso foi a investigação de secretária, as fontes de informação específicas podem ser encontradas na secção referências deste documento.

PREVENIR

☑ **Práticas que não tiveram efeito:** Autenticação no site - De forma a acompanhar a sua encomenda de roupa, o utilizador recebeu um link para iniciar sessão como convidado no site. O utilizador convidado tinha amplos direitos de obter informações para as encomendas feitas por todos os outros utilizadores apenas alterando o URL do hóspede. Por isso, a base de dados foi comprometida através do website uma vez que não pedia autenticação e considerava o utilizador convidado um utilizador válido. Os dados visíveis para outros clientes consistiam em nomes, últimos dígitos dos seus cartões de crédito, morada, número de telefone, etc.

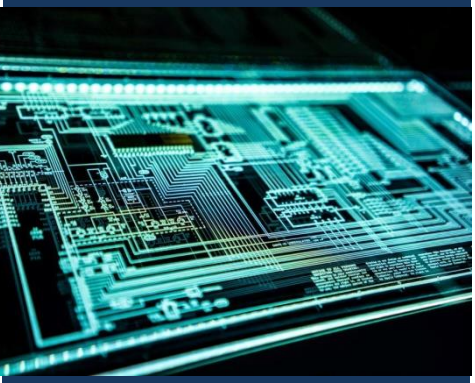
☑ **Práticas que tiveram efeitos comprovados em verdadeiros ciberataques deste tipo:**

1. Descoberta da exposição aos dados (utilizando sistemas de digitalização externos).
2. Autenticação forte (Log-in único permitindo que um utilizador entre em vários sistemas ou utilizadores/palavras-passe diferentes para cada sistema).
3. 3. Priorização do acesso aos dados (por exemplo, os RH só podem necessitar de acesso à informação dos empregados e o departamento contabilístico só pode necessitar de acesso aos dados orçamentais e fiscais. Os utilizadores convidados devem ter acesso mínimo de dados).

4. Implantação de infraestruturas de monitorização e soluções automatizadas que podem identificar rapidamente potenciais problemas antes de se tornarem emergências, isolar bases de dados infetadas e sinalizar para apoiar e equipas de TI para os próximos passos.

IDENTIFICAR

O ataque contra a Hanesbrands Inc. foi de **Divulgação de informação**.



Na última semana de junho e no primeiro de julho de 2015 Hanesbrands Inc. foi vítima de ciberataque. Após o roubo dos dados, a empresa foi informada pelos adversários sobre a violação sem dar um motivo para a sua ação. É muito provável que a fraqueza da empresa tenha sido descoberta através da digitalização[1]. Os hackers criaram uma encomenda de check-out "guest" no site da Hanesbrands[2] (sem sequer se registarem no site). Com o link de encomendas recebido, os hackers conseguiram esvaziar a base de dados da empresa que era responsável pela detenção de dados para todas as encomendas dos clientes (encomendas que eram feitas no seu website ou através do telefone) – como se verificou que o link de check-out "convidado" era capaz de aceder a todas as outras encomendas sem autenticação. Numa semana, os adversários conseguiram obter informações para mais de 900 000 clientes. Para não serem detetados, os hackers provavelmente usaram o Port Knocking[3] para ocultar a sua atividade. De acordo com Hanesbrands, os adversários usaram screenshots[4] para extrair os dados, no entanto é muito provável que tenham usado uma forma mais automatizada – como o script que analisa os dados diretamente[5].

O ataque descrito pelo modelo MITRE ATT&CK:
[1] Digitalização ativa: Digitalização da vulnerabilidade (T1592.002)." 2] Acesso inicial: Explorar aplicação virada para o público (T1190).
[3] Persistência: Sinalização de tráfego: Batida portuária (T1205.001).
[4] Captura de Ecrã (T1113).
[5] Coleção Automatizada (T1119).

O ataque foi identificado pela empresa depois de ter sido notificado pelos adversários. Hanesbrands não sabia que isto estava a acontecer até que os hackers os informassem.

RESPONDER

Em junho de 2015 , a Hanesbrands Inc. foi informada pelos adversários sobre a violação. Através da conta de hóspedes no seu site, os atacantes conseguiram extrair informações gerais dos utilizadores para 900.000 clientes. Depois de ter sido notificado sobre a fuga, a Hanesbrands

adicionou a autenticação à sua base de dados de "encomendas de clientes" e removeu a opção de "check-out" (apesar de a terem corrigido).

QUEM: Desconhecido.

A QUEM: Hanesbrands Inc.

PORQUÊ: It was a targeted attack to obtain information on customer database & clients' lists but no ransom was requested by the adversaries after all. They just informed Hanesbrands that they obtained the data.

O QUÊ: Informação geral do cliente para 900.000 clientes – nomes, moradas, informações sobre o estado da encomenda do cliente, números de telefone e os últimos 4 dígitos do seu Cartão de Crédito. Mas os nomes de utilizador ou palavras-passe dos clientes não foram divulgados. Os hackers não comprometeram os sistemas corporativos de Hanesbrands.

COMO: Os adversários criaram uma encomenda através do check-out da conta de hóspedes no site da Hanesbrands. Fazendo-se passar por um "convidado" que está a verificar uma ordem (os adversários não estavam registados no site) conseguiram encontrar uma violação na base de dados de Hanesbrands explorando o link da encomenda. Os hackers conseguiram aceder aos dados e estado das encomendas dos clientes e extrair os dados durante cerca de uma semana utilizando a opção "explorar com check-out" no site.

ESTRATÉGIA: Assim que Hanesbrands foi notificado sobre a violação pelos adversários, eles adicionaram autenticação à sua base de dados para parar o buraco de divulgação de informação. Além disso, repararam o check-out do "utilizador convidado" através do qual a fuga foi gerida. A Hanesbrands notificou os seus clientes sobre a violação por e-mail e correio. Desde o acidente, a Hanesbrands está a investir cada vez mais na cibersegurança a cada ano.

RECUPERAR

☑ **IMPACTO:** As consequências foram a fuga de informação geral do cliente. Não é revelado de quaisquer processos ou outros danos diretos.

☑ **ESTRATÉGIA DE RECUPERAÇÃO:** Hanesbrands informou os seus clientes sobre a violação. Reparámos o link "utilizador convidado"[1] a fim de não ter acesso direto à base de dados e desativá-lo globalmente como opção[2]. Ofereceram serviço ao cliente para responder se os utilizadores têm preocupações. Além disso, realizou auditorias de segurança[3] e análise de vulnerabilidade[4] aos seus sistemas existentes e investiu em formações de cibersegurança[5].

☑ As mitigações descritas pelo modelo MITRE ATT&CK:
[1] Configuração de software (M1054).
[2] Desativar ou remover recurso ou um programa (M1042).
[3] Auditoria (M1047).
[4] Digitalização da vulnerabilidade (M1016).
[5] Orientação do Desenvolvedor de Aplicações (M1013).

☑ **MELHOR ESTRATÉGIA:** Depois de reparar o link "utilizador convidado" através do qual um cliente poderia rever a sua compra, a Hanesbrands está a desativar isso como uma opção. Em vez disso,

poderiam ter adicionado um controlo para atividades suspeitas e/ou políticas para rever apenas determinado montante de compras.

LIÇÕES APRENDIDAS

Os ataques de divulgação de informação tornam-se muito raros, uma vez que muitas ferramentas modernas fornecem segurança cibernética automática neles e aconselham as empresas sobre o que poderia ser uma possível fuga. O ataque a Hanesbrands mostra que a fraca pista de auditoria da base de dados e a falta de conhecimentos de segurança podem ser facilmente exploradas. Em muitos casos, as bases de dados são violadas devido ao nível insuficiente de conhecimentos especializados em cibersegurança e à falta de formação/educação relevante de funcionários não técnicos que, consequentemente, podem quebrar as regras básicas de segurança da base de dados. O pessoal das TI também poderia não ter os conhecimentos necessários para impor as políticas de segurança, realizar processos e ações de relatórios de incidentes adequados.

Outro ponto é que a base de dados em Hanesbrand estava vulnerável devido a uma má configuração – as bases de dados geralmente ficam totalmente desprotegidas por causa disso. Muitas vezes esquece-se que normalmente os adversários são especialistas em TI altamente profissionais, que certamente sabem explorar tais vulnerabilidades. Isto pode ser contrariado desativando as contas de base de dados padrão combinadas com pessoal de TI treinado e experiente.

Hanesbrands teve sorte de que apenas foram divulgadas informações gerais, bem como que os adversários informaram a empresa depois de extrair todos os dados que podiam. Além disso, a Hanesbrands informou imediatamente os seus clientes pela violação que mostra que a empresa quer ser frontal com os seus clientes, e a questão está a ser levada a sério.

"A falsificação (spoofing) é uma técnica de ataque que se baseia na falsificação de dados numa rede de forma a permitir que um site malicioso ou comunicação disfarçam-se de confiança." (O Glossário Cyberwire, N.D.)

ESTUDO DE CASO 5: FALSIFICAÇÃO HUMANA

ORGANIZAÇÃO DIRECIONADA

Humana é uma companhia de seguros de saúde sediada em Louisville. Fundada originalmente em 1961 como operadora de lares de idosos, a principal atividade da empresa passou a possuir e gerir hospitais, depois para planos de seguro de saúde na década de 1980. Em maio de 2015, a Forbes estimou que a empresa valeria 26,7 mil milhões de dólares. Em 2020, a Humana teve uma receita de 77,155 mil milhões de dólares e cerca de 48 mil colaboradores. Mensalmente, Humana é gastando mais de $100.000 em cibersegurança. A Humana está a usar produtos de cibersegurança como "Akamai" (plataforma de entrega em nuvem) e "Prolílico (soluções de segurança para proteger sites, dados centros, e aplicações IP empresariais de ataques de Negação de Serviço Distribuído

(DDoS)", "Proofpoint" (solução para proteger as pessoas e dados críticos de ameaças avançadas de e-mail), programas "Alert Logic" (deteção e resposta geridas por luva branca) e outros.

COMO A INFORMAÇÃO FOI ADQUIRIDA?

O método aplicado para recolher as informações para este estudo de caso foi a investigação de secretária, as fontes de informação específicas podem ser encontradas na secção referências deste documento.

PREVENIR

☑ **Práticas que não tiveram efeito:** Alertas para tentativas falhadas de login – Humana aplicou esta prática antes do incidente. Não foi eficaz, uma vez que a organização demorou aproximadamente um dia a tomar medidas em resposta às numerosas tentativas falhadas de login recebidas.

☑ **Práticas que tiveram efeitos comprovados em verdadeiros ciberataques:**

1. Bloqueio de conta após tentativa falhada de login.
2. Bloquear o tráfego de internet de países estrangeiros com os quais a organização não faz negócios.
3. Forçar uma redefinição de senha.

IDENTIFICAR

O ataque contra Humana foi de **falsificação.**

No dia 3 de junho de 2018, a Humana foi alvo de um sofisticado ataque de falsificação cibernética que ocorreu no Humana.com. No mesmo dia, a Humana tomou conhecimento de um aumento significativo das tentativas de erro de login dos endereços IP de países estrangeiros[1]. Para não revelarem a sua localização real, os adversários utilizaram proxies multi-hop[2]. O volume das tentativas de login para Humana.com sugeriu que um ataque grande e amplo foi lançado. A natureza do ataque e os comportamentos observados indicavam que o intruso tinha uma grande base de dados de identidades de utilizador e senhas correspondentes que estavam a ser inseridas com a intenção de identificar quais poderiam ser válidas em Humana.com por "força bruta"[3]. O número excessivo de erros de login sugere que as informações credenciais não provêm da Humana[4] (e muito provavelmente foram compradas na teia "escura"). No dia 4 de junho, a Humana bloqueou os IP. Com base nestes factos, isto pode ser descrito como um ataque de falsificação de identidade. Os

adversários recolheram dados[5] de cerca de 65 000 utilizadores que incluem:

- ☑ Reclamações médicas, dentárias e de visão, incluindo serviços realizados, nome do prestador, datas de serviço, encargos e valores pagos, etc.
- ☑ Informação sobre contas de despesas, como despesas com contas de poupança de saúde e informação sobre saldos.

Após o incidente, a Humana tomou medidas adicionais como bloqueio de conta após tentativa falhada de login, bloquear o tráfego de internet de países estrangeiros com os quais a organização não faz negócios e forçar um reset de senha.

O ataque descrito pelo modelo MITRE ATT&CK:
[1] Intérprete de Comando e Script: Dispositivo de Rede CLI (T1059.008).
[2] Proxy: Multi-hop Proxy (T1090.003).
[3] Força Bruta: Recheio Credencial (T1110.004).
[4] Recolher informações sobre a identidade da vítima: credenciais (T1589.001).
[5] Coleção Automatizada (T1119).
O ataque foi identificado por alertas de vários erros de login.

RESPONDER

- ☑ **QUEM:** Desconhecido
- ☑ **A QUEM:** Humana
- ☑ **PORQUÊ:** Roubo de identidade (provavelmente vendida a terceiros)
- ☑ **O QUÊ:** Informações sensíveis dos utilizadores (reclamações médicas, dentárias e de visão, incluindo serviços realizados, nome do prestador, datas de serviço, encargos e valores pagos, etc; informações sobre contas de despesas, tais como despesas com contas de poupança de saúde e informações sobre saldo)
- ☑ **COMO:** Os adversários recolheram grandes quantidades de contas e credenciais. Em seguida, usando proxies multi-hop que forçam login com as contas que tinham. Após login bem sucedido os adversários recolhem os dados de utilizadores através de pequenas transferências de dados.
- ☑ **ESTRATÉGIA:** Assim que a Humana notou o aumento significativo do número de erros de tentativas de login, os seus operadores de cibersegurança bloquearam os endereços IP estrangeiros a partir dos quais foram feitas as múltiplas tentativas de login. Depois disso, a Humana forçou o reset da palavra-passe em todas as contas conhecidas por terem sido violadas e até lançou um produto - oferecendo aos membros uma proteção de roubo de identidade durante um ano.

RECUPERAR

- ☑ **IMPACTO:** A consequência foi a fuga de informações confidenciais dos utilizadores (alegações médicas, dentárias e de visão, incluindo serviços realizados, nome do prestador, datas de serviço, encargos e montantes pagos, etc; informação sobre contas de despesas, como despesas com poupanças de saúde e informações sobre saldos). Muitos processos por negligência foram arquivados em relação à Humana depois disso. Não há informação se os processos foram ganhos pela empresa, o que sugere que os resultados foram provavelmente negativos.

☑ **ESTRATÉGIA DE RECUPERAÇÃO:** A Humana notificou o número de membros para os informar sobre a violação de dados após um mês de aprovação. Tomaram igualmente uma série de medidas para aumentar a sua segurança cibernética, incluindo: 1) forçando a reposição da palavra-passe[1]; 2) implantação de novos alertas para logins bem sucedidos e falhados[2] e 3) contas bloqueadas ligadas a atividades suspeitas[3]. Além disso, implementaram uma série de controlos técnicos para melhorar a segurança do portal web (bloco de ataque de força bruta, defesa de injeção SQL[4], instalação de um certificado de segurança SSL[5], etc.). A empresa bloqueou igualmente todos os endereços IP estrangeiros que não eram relevantes para as suas operações[6].

As mitigações tomadas pela Humana descritas pelo modelo MITRE ATT&CK:

[1] Políticas de senha (M1027).
[2] Prevenção da Intrusão em Rede (M1031).
[3] Políticas de Utilização de Conta (M1036).
[4] Configuração de software (M1054).
[5] Inspeção SSL/TLS (M1020).
[6] Tráfego da rede de filtros (M1037).

☑ **MELHOR ESTRATÉGIA:**

A Humana podia ter notificado os utilizadores mais cedo. Também poderiam ter adicionado medidas de segurança adicionais, tais como:

- Utilização da autenticação com base na troca de chaves entre as máquinas na rede de uma organização ou na autenticação de vários fatores para acesso remoto;
- Utilizar uma lista de controlo de acesso para negar endereços IP privados em interfaces a jusante;
- Aplicação da filtragem do tráfego de entrada e saída;
- Configurar routers e comutadores - se possível - para rejeitar pacotes originários de fora da rede local de uma organização que alega ter origem a partir de dentro;
- Ativar sessões de encriptação no router de uma organização para que os anfitriões confiáveis fora da sua rede possam comunicar de forma segura com os seus anfitriões locais.

LIÇÕES APRENDIDAS

As lições aprendidas poderiam ser identificadas como a necessidade de colocar mais foco na obtenção de dados pessoais dos utilizadores, organizar formações do pessoal para sensibilizar para as ameaças cibernéticas, notificar os utilizadores de dados de fuga devido aos inúmeros processos de negligência em relação à Humana após o incidente (a Humana não divulgou qualquer informação de que tal ataque tenha ocorrido até um mês depois).

Os efeitos do ataque não estavam apenas ligados às despesas para lidar com o ataque e os processos judiciais, mas também com os grandes danos à reputação da Humana e à sua fiabilidade. Uma vez que a empresa está no domínio dos seguros de saúde, é crucial que tenha as mais elevadas medidas de segurança e confiança dos seus clientes, uma vez que os dados armazenados nos seus sistemas são muito sensíveis e confidenciais. É por isso que a Humana era e continua um alvo de topo para

ciberataques muito antes do especificado neste caso e também depois. Tendo em conta isto, o erro no julgamento da gravidade deste ataque pode ser considerado surpreendente.

ESTUDO DE CASO 6: NEGAÇÃO DE SERVIÇO WILLIAM HILL

ORGANIZAÇÃO ALVO

William Hill é uma empresa de jogos de apostas online com sede em Londres, Inglaterra - fundada originalmente em 1934 por William Hill. A empresa mudou de mãos muitas vezes – foi comprada pela primeira vez em 1971 pela Sears Holdings. Depois de ter sido vendido inúmeras vezes em abril de 2021, foi adquirido pela Ceasars Entertainment. Em 2020, a empresa teve receitas de 1.324,3 milhões de libras e 12.000 colaboradores (8.000 no Reino Unido) em 2021.A empresa tinha mais de 1400 lojas de apostas, mas em 2019 começou a fechar mais de 800 lojas devido aos baixos lucros, mas alegando que manteria o seu pessoal intacto.

Mensalmente, o William Hill está a gastar mais de $100.000 para a segurança cibernética. A empresa está a usar produtos de cibersegurança como "Prolexic" (soluções de segurança para proteger sites, centros de dados e aplicações IP empresariais de ataques de Negação de Serviço Distribuído (DDoS)", "Proofpoint" (solução para proteger as pessoas e dados críticos de ameaças avançadas de e-mail), "F5 BIG-IP Application Security Manager" (firewall de aplicação web flexível que garante aplicações web em aplicações web tradicionais, ambientes em nuvem virtual e privada) , "Check Point" (protege os seus clientes de ciberataques de 5ª geração com uma taxa de captura líder da indústria de malware, ransomware e ameaças avançadas direcionadas), etc.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

O método aplicado para recolher as informações para este estudo de caso foi a investigação literária, as fontes de informação específicas podem ser encontradas na secção referências deste documento.

PREVENIR

☑ **Práticas que não tiveram efeito:**

1. Qualquer difusão de rede – William Hill tem este tipo de defesa – que é útil para conter enormes quantidades de clientes que visitam o seu website ou podem dissolver enormes quantidades de tráfego de rede indesejado (como o ataque DDoS). Essa estratégia normalmente funciona para a maioria dos casos de ataques de DDoS.
2. O simples aumento da largura de banda da rede (o tráfego que pode reter) não provou ser eficaz neste ataque.

☑ **Práticas que tiveram efeitos comprovados em verdadeiros ciberataques deste tipo:**

1. Implementação de proteção DDoS ao nível do servidor – regras adicionais que ajudam a identificar e bloquear o tráfego de rede malicioso.

2. Adicionando 3ª parte A difusão da rede Anycast – isto pode ajudar as empresas a aumentar tremendamente a sua capacidade de assumir muito mais tráfego de rede ou lidar com ataques DDoS.

IDENTIFICAR

O ataque contra William Hill foi de **negação de serviço.**

Em 1 de novembro de 2016, William Hill foi alvo de um ataque de negação de serviço distribuído por alto desempenho[1]. Antes do ataque, os adversários recolheram informações sobre os detalhes da rede de william Hill[2]. Depois disso, os adversários inundaram o site de William Hill com tráfego para que não pudesse funcionar corretamente.O ataque negou aos clientes a aposta nos jogos da UEFA Champions League de terça-feira à noite. O ataque a William Hill foi conseguido com a ajuda de um malware chamado "Mirai"[4], que cria uma rede de numerosos sistemas informáticos que é conhecido como "botnet"[3] para iniciar o ataque do DDoS através deles.

"De acordo com a Cloudflare, no 4º trimestre de 2021 a indústria transformadora recebeu mais ataques DDoS em camadas de aplicação, registando um aumento de 641% no número de ataques." (Cook, 2022)

O ataque descrito pelo modelo MITRE ATT&CK :
[1] Rede Negação de Serviço: Inundação de rede direta (T1498.001).
[2] Recolher informações sobre a rede de vítimas: endereços IP (T1590.005).
[3] Adquirir Infraestrutura: Botnet (T1583.005).
[4] Vírus worm auto-propagador que utiliza base de dados de credenciais padrão. Com estas credenciais, os dispositivos IoT (dispositivos inteligentes como rastreadores de fitness, assistentes de voz, acessórios smarthome, etc.) são digitalizados e infetados.

O ataque foi identificado logo após o site de William Hill ficar sem resposta e deixar de ser acessível.

RESPONDER

QUEM: Desconhecido.
A QUEM: William Hill.
PORQUÊ: Disputas empresariais – é muito provável que o rival da empresa faça tais ações especialmente em tempo de eventos desportivos populares como a UEFA Champions League / Extortion – se William Hill não conseguir lidar com a situação é provável que o resgate seja solicitado.
O QUÊ: O site de William Hill foi para baixo por 24 horas, o que causou perdas de 4,4 milhões de libras. Levou dias para William Hill restaurar o seu site e sistemas totalmente.
COMO: No site de William Hill foi realizado ataque de Negação de Serviço Distribuído de Alto Desempenho com rede "botnet" (múltiplos computadores que foram infetados pelo vírus malware e usados para

realizar tal ataque sem o seu conhecimento ou consentimento) criado por um malware chamado "Mirai".

ESTRATEGIA: Depois de notar que o seu website está em William Hill, os especialistas em TI começaram a filtrar o tráfego que está a chegar. William Hill usou a difusão da rede Anycast – enviando tráfego de rede espalhando-o por rede de servidores da empresa. Esta mitigação distribui o tráfego da rede ao ponto de o tráfego ser absorvido pela rede da empresa. Esta estratégia de utilidade depende do tamanho da rede da empresa e do tamanho do ataque do DDoS. No caso de William Hill – mesmo com a sua infraestrutura de topo e segurança não foram suficientes para lidar com tal ataque.

RECUPERAR

IMPACTO: O ataque do DDoS contra William Hill fez com que o seu site permanecesse em baixo por mais de 24 horas em que os clientes não podiam apostar nos jogos da Liga dos Campeões da UEFA. Isso resultou em perdas superiores a 4,4 milhões de libras num só dia. Felizmente para William Hill apenas o seu website foi direcionado para manter intactos os dados sensíveis dos seus utilizadores (o que é uma pista de que os adversários queriam negar aos utilizadores de visitar o website, e não roubar dados). Demorou mais de 4 dias a trabalhar 24 horas por dia para os especialistas em TI de William Hill reavivarem o seu website e sistemas afetados.

ESTRATÉGIA DE RECUPERAÇÃO: Para enfrentar o ataque, William Hill filtrava o tráfego da rede de entrada[1]. Filtrar o tráfego da rede – bloqueando o tráfego apenas de ataque e permitindo um legítimo. Também começaram a utilizar fornecedores de difusão de rede Anycast 3 rd (empresas que estão a oferecer este tipo de serviço – que dissolve o ataque DDoS ao dispersar todo o tráfego de entrada através da sua rede).

MELHOR ESTRATÉGIA:

☑ Verificação sanitária de hospedeiro, que alertará os especialistas em TI da empresa quando for detetada uma utilização anormal da rede [2]. Se for detetado a tempo, podem ser tomadas medidas para ajudar a manter o serviço do site disponível.

☑ Pode ser utilizado "encaminhamento do buraco negro". É uma técnica que canaliza tanto o tráfego legítimo como o tráfego malicioso, para uma rota nula e abandonou a rede. Não é uma solução ideal, pois torna o site inacessível.

☑ Limitação de taxas. Limita o número de pedidos que o servidor pode receber – por si só não consegue parar o ataque do DDoS, mas é uma ferramenta útil na estratégia de defesa global.

A estratégia de recuperação descrita pelo modelo MITRE ATT&CK:

a. [1] Filtro de Tráfego de rede (M1037).
b. [2] Saúde dos sensores: Estado do hospedeiro (DS0013).

LIÇÕES APRENDIDAS

O ataque contra William Hill pode mostrar-nos que mesmo uma empresa com uma segurança cibernética excecional e que está preparada para lidar com estes ataques pode sofrer com eles.

Apesar de o seu website ter sido retirado pelo ataque do DDoS (normalmente tais ataques são apenas uma cortina de fumo para o ataque real), a segurança de alto nível da empresa estava intacta e funcional, mantendo as informações sensíveis dos clientes seguras. Isso mostrou aos seus clientes que estão seguros e mantiveram a credibilidade da empresa. Dado que os adversários não tentaram explorar a vulnerabilidade de William Hill, pontos que provavelmente o ataque foi feito devido à rivalidade comercial (empresa concorrente que quer aproveitar o mercado de apostas) ou a uma tentativa de extorsão (a empresa depende do seu website, e mantê-lo baixo por adversários gera perdas).

Com a entrada na era dos dispositivos inteligentes (IoT) quando tudo pode ser operado remotamente (luzes inteligentes, aspiradores, frigoríficos, relógios inteligentes, etc.), também temos de pensar na segurança que precisa de ser aplicada. Todos estes dispositivos inteligentes têm endereço IP, e podem ser pirateadosnarede – para obter informações ou "zombified" (o seu dispositivo está a ser controlado sem que você saiba e comece a funcionar de forma estranha) e usado em ataques DDoS para inundar um website.

ESTUDO DE CASO 7: COBALT STRIKE: O USO DE FERRAMENTAS DE TEAMING VERMELHAS POR CRIMINOSOS VIRTUAIS

ORGANIZAÇÃO ALVO

Cobalt Strike é uma ferramenta de equipa vermelha que foi desenvolvida em 2012. O seu principal objetivo é ajudar as equipas vermelhas a testar e simular ciberataques. Como a ferramenta tem boas capacidades para contornar os limites de segurança através de evasões, os atacantes sequestraram algumas das suas versões para abusar dela como uma ferramenta de entrega de cargas maliciosas, como o ransomware. Este estudo de caso não se centra numa única organização, uma vez que a Cobalt Strike é utilizada na natureza para realizar ataques em massa dirigidos a vários tipos de organizações, tais como manufactories, instituições financeiras, empresas de telecomunicações, entre outras.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

O método aplicado para recolher as informações para este estudo de caso foi a investigação de secretária, as fontes de informação específicas podem ser encontradas na secção referências deste documento.

PREVENIR

A deteção e prevenção de um ataque que faz uso da ferramenta de teaming vermelha Cobalt Strike envolve uma cadeia de segurança em toda a infraestrutura completa. Isto começa já com software de proteção e monitorização no cliente de ponto final e vai até ao nível da rede. Além disso, a inteligência de ameaças ativas também é necessária para manter as ferramentas de deteção baseadas em assinaturas atualizadas.

Isto normalmente envolve:

- ☑ Segurança no ponto final (como antivírus, monitorização baseada no hospedeiro)
- ☑ Segurança da rede (como firewall, proxy, deteção de assinaturas/padrões no tráfego)
- ☑ Segurança de e-mail
- ☑ Políticas corretas de anfitrião/segurança configuradas

IDENTIFICAR

Cobalt Strike é uma ferramenta comercial multifuncional que cumpre diferentes técnicas de ataques. Considerando a ferramenta e as suas próprias capacidades, pode ser classificada como divulgação de informação e elevação de privilégios. No entanto, como também pode ser usado para deixar cair ainda mais cargas maliciosas, especialmente porque os ataques de ransomware foram observados em combinação com cobalto strike, a lista pode ser estendida com Adulteração e Negação de Serviço.

Tendo em conta todas as funcionalidades da ferramenta, trata-se de uma ferramenta de acesso remoto com capacidades de movimento lateral. Isto leva a uma enorme lista de técnicas de ataques usadas pela Cobalt Strike, e, portanto, só vamos cobrir alguns deles aqui.

- ☑ Mecanismo de Controlo de Elevação de Abuso (T1548) Uma vez que a Cobalt Strike foi executada num sistema, tem a capacidade de executar várias técnicas usadas para obter permissões mais elevadas.
- ☑ BITS Jobs (T1197) BITS é uma ferramenta windows que pode ser usada pela Cobalt Strike para descarregar cargas
- ☑ Intérprete de Comando e Scripting (T1059) Cobalt Strike pode usar várias ferramentas para executar comandos, códigos e scripts. Isto inclui PowerShell, Windows Command Shell, Visual Basic, Python e JavaScript.

- ☑ Exploração para Escalada de Privilégios (T1068) Para obter privilégios mais elevados, a Cobalt Strike pode explorar vulnerabilidades dentro do sistema operativo.
- ☑ Captura de entrada (T1056)/Captura de Ecrã (T1113) Cobalt Strike também pode funcionar como um keylogger e recolher imagens do sistema infetado.

RESPONDER

- ☑ **QUEM:** Desconhecido
- ☑ **A QUEM:** Várias organizações em todo o mundo
- ☑ **PORQUÊ:** Cobalt Strike foi usado em várias campanhas focando-se em objetivos diferentes. Na razão do ataque é ter acesso à rede de organização interna para movimentos laterais. Outra razão poderá ser causar danos às empresas, atacando a rede comprometida com, por exemplo, um ransomware.
- ☑ **O QUÊ:** Principalmente para acesso remoto, compromisso de rede e movimento lateral.
- ☑ **COMO:** Cobalt Strike é uma ferramenta de equipa vermelha comercial usada para simular ciberataques que foram sequestrados. A ferramenta é usada para obter o acesso inicial a uma rede da empresa, bem como para outras ações com a rede comprometida.
- ☑ **ESTRATÉGIA:** Dependendo da empresa atacada, a informação sobre como identificaram e reagiram ao ataque é desconhecida.

RECUPERAR

- ☑ **IMPACTO:** O intruso pode obter acesso total à rede dentro da empresa. Isto pode levar à divulgação de informação, bem como a novos ataques que são entregues dependendo do operador do ataque.
- ☑ **ESTRATÉGIA DE RECUPERAÇÃO:** Dependendo da empresa atacada, a informação de como a sua estratégia de recuperação parecia é desconhecida.
- ☑ **MELHOR ESTRATÉGIA:**
  - Mantenha os sistemas antivírus atualizados
  - Utilizar sistemas de deteção e prevenção de intrusões de intrusões
  - Monitorizar adequadamente os sistemas para atividades suspeitas
  - Configurar adequadamente sistemas e desativar os serviços não necessários
  - Conhecimento de formação dos colaboradores
  - Utilize a segmentação a nível de rede e limite a comunicação permitida a um mínimo exigido

LIÇÕES APRENDIDAS

Embora seja necessário construir ferramentas vermelhas de teaming que podem ser usadas para simulação de ataque numa rede para encontrar possíveis pontos vulneráveis, ainda é preciso ter em mente que essa ferramenta também pode ser comprometida e usada por um intruso.

ESTUDO DE CASO 8: ZERO DIAS DE ATAQUE - GRUPO DE HACKERS HAFNIUM ALVO DE TROCA DE SERVIDORES

ORGANIZAÇÃO ALVO

No início de 2021, os investigadores encontraram múltiplas vulnerabilidades críticas no Microsoft Exchange Server, o que levou a uma exploração massiva em todo o mundo. As vulnerabilidades foram usadas na natureza por várias organizações criminosas, nomeadamente o grupo HAFNIUM, antes de os patches serem fornecidos pela Microsoft. Isto fez com que os ataques especialmente difíceis de responder e de recuperar.

COMO A INFORMAÇÃO FOI ADQUIRIDA?

O método aplicado para recolher as informações foi a revisão de literatura, as fontes de informação específicas podem ser encontradas na secção referências deste documento.

PREVENIR

Dezenas de milhares de empresas foram afetadas por este ataque. Devido à exposição geral dos Microsoft Exchange Servers à internet e ao potencial de bypass de autenticação do ataque, foi muito difícil de prevenir em primeiro lugar. Isto leva ainda a suposição de que as diferentes práticas de segurança aplicáveis a essas empresas não tiveram qualquer impacto.

IDENTIFICAR

Há quatro vulnerabilidades diferentes que levaram aos ataques descritos. As vulnerabilidades são **CVE-2021-26855, conhecido como "ProxyLogon", CVE-2021-27065, CVE-2021-26857 e CVE-2021-26858**. A técnica para explorar estas vulnerabilidades é descrita como **"Exploração para Execução de Clientes" (T1203)** no âmbito do MITRE ATT&CK.

CVE-2021-26855 é um bypass de autenticação utilizando o representante interno do Servidor de Câmbio. Com isto, um intruso pode ter acesso privilegiado ao próprio Servidor. Combinando-o com outra vulnerabilidade como o CVE-2021-27065, que permite escrever ficheiros arbitrários no sistema, ou CVE-2021-26857, para obter acesso ao SISTEMA (T1078) através de uma deserialização insegura, cria uma cadeia de exploração sem restrições.

Os ataques ocorreram na natureza antes que a Microsoft pudesse lançar um patch para as vulnerabilidades. De acordo com inúmeros recursos, este período era de cerca de 58 dias de exploração de zero dias. O primeiro grupo que estava associado a estas vulnerabilidades foi o HAFNIUM. Mais

tarde, vários outros grupos começaram a abusar destas vulnerabilidades. As capacidades do ataque permitiram vários cenários, desde a exfiltração de dados (T1567) até à implementação do ransomware (T1486).
Segue-se uma lista de ações tomadas pelo grupo HAFNIUM usando este vetor de ataque:

☑ T1589 – Recolha de endereços de e-mail para utilizadores que pretendiam atingir

☑ T1071 – quadro C2 de código aberto (por exemplo, pacto)

☑ T1560 – 7-Zip, WinRAR para comprimir ficheiros roubados para extração

☑ T1059 – Exportar dados da caixa de correio via PowerShell

☑ T1567 – Exfiltrar dados através de sites de partilha, incluindo MEGA

☑ T1105 – Descarregar malware e ferramentas em anfitriões comprometidos (por exemplo, Nishang, PowerCat)

☑ T1003 – Dumping credencial de LSASS e bases de dados de diretório ativo (NTDS.DIT)

☑ T1505 – Implantação de WebShells em anfitriões comprometidos (SIMPLESEESHARP, SPORTSBALL, etc.)

A identificação dos ataques pode ocorrer devido à inspeção de registo em possíveis máquinas comprometidas. Microsoft divulgou orientações sobre a deteção de todas as vulnerabilidades de acordo com o seu Indicador de Compromisso.

RESPONDER

QUEM: HAFNIUM (grupo provavelmente patrocinado pelo Estado com ligações à China)
A QUEM: Diferentes empresas em todo o mundo, principalmente a indústria dos EUA
PORQUÊ: Exfiltração de dados e provavelmente ganhar dinheiro através de ransomware
O QUÊ: Conhecimentos da empresa tais como dados, endereços de e-mail, caixas de correio
COMO: Aproveitando múltiplas vulnerabilidades no Microsoft Exchange Server para permitir a execução de código remoto não autenticado
ESTRATÉGIA: Digitalizar a gama IP da internet para recolher listas IP dos Servidores de Troca do Microsoft. Explorando as vulnerabilidades mencionadas para implantar web shell ou C2 beacon. A utilização deste acesso permitiu comprimir e exfiltrar dados através de sites de partilha online como o MEGA. Ocasionalmente, implementando ransomware "DearCry". Isto foi possível devido à disponibilidade tardia do patch e má gestão de patch de empresas.

RECUPERAR

IMPACTO: As consequências deste ataque podem ser consideradas como perda de informação, uma vez que tanto a exfiltração como o ransomware se enquadram nesta categoria. Além disso, se as organizações tentaram pagar o resgate para recuperar os seus dados, também acabaram com um dano financeiro.

ESTRATÉGIA DE RECUPERAÇÃO: Dependendo do ataque específico, a recuperação pode diferir. O processo de recuperação de um ransomware pode demorar muito tempo. Todos os sistemas infetados devem ser reinstalados ou uma cópia de segurança tem de ser revertida. Se as cópias de segurança foram armazenadas num sistema infetado, obviamente não podem ser usadas para o processo de recuperação. A recuperação da exfiltração de dados é diferente. No início , devem ser aplicadas manchas disponíveis e devem ser removidos vestígios de conchas web ou balizas C2. É importante avaliar qual, e quantos dados foram roubados para medir o impacto.

MELHOR ESTRATÉGIA

- ☑ Mantenha os sistemas antivírus atualizados
- ☑ Utilizar sistemas de deteção e prevenção de intrusões de intrusões
- ☑ Monitorizar adequadamente os sistemas para atividades suspeitas
- ☑ Configurar adequadamente sistemas e desativar os serviços não necessários
- ☑ Gestão de patch rápido para corrigir vulnerabilidades o mais rápido possível
- ☑ Utilize a segmentação a nível de rede e limite a comunicação permitida a um mínimo exigido

LIÇÕES APRENDIDAS

A exploração zero-dia com correntes de ataque parece muito intimidante. A chave para enfrentar estes desafios é uma segmentação adequada da rede e monitorização do sistema para identificar possíveis ataques em tempo útil. Os sistemas de intrusão e prevenção da rede também podem ajudar a detetar tais ataques. O que também é importante é que os patches para vulnerabilidades críticas devem ser aplicados o mais rapidamente possível para remediar ainda mais os vetores de ataque.
Como outra lição aprendida, quero mencionar os investigadores de segurança da DevCore que primeiro detetaram as vulnerabilidades e ajudaram com a Microsoft no processo de patch. Isto reforça a importância da investigação de segurança independente para a boa causa.

ESTUDO DE CASO 9: WannaCry: QUANDO UM RANSOMWARE PARALISA O SISTEMA DE SAÚDE

ORGANIZAÇÃO ALVO

Já em 2017, um novo ransomware chamado **WannaCry (WannaCrypt)** que visa o sistema operativo Windows infetou milhares e milhares de clientes em todo o mundo. Em vez de visar uma organização específica, o ataque foi generalizado e afetou muitas empresas dentro de diferentes áreas.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

O método aplicado para recolher as informações para este ESTUDO DE CASO foi a investigação de secretária, as fontes de informação específicas podem ser encontradas na secção referências deste documento.

PREVENIR

Várias empresas foram afetadas por este ataque, o que leva ao pressuposto de que as diferentes práticas de segurança que se aplicam a essas empresas não tiveram qualquer impacto.

IDENTIFICAR

O WannaCry é uma aplicação maliciosa que é classificada como **ransomware** , uma vez que encripta ficheiros específicos dos utilizadores num sistema direcionado. Isto leva à adulteração de dados e à sua destruição, uma vez que o proprietário do sistema infetado não é capaz de desencriptar os ficheiros. Isto termina posteriormente num ataque de negação de serviço devido aos ficheiros e dados em falta.

Uma das principais características do WannaCry é a sua técnica utilizada para pesquisar automaticamente os potenciais sistemas-alvo que o ransomware tenta também infetar. Como este malware pode infetar outros sistemas de um já infetado, também é referido como um worm. Para atingir este objetivo, uma exploração para vulnerabilidade de software no protocolo SMB do Microsoft Windows chamado Eternal Blue é usado e mapeia o MITRE ATT&CK ID T1210.

Antes que o malware possa espalhar e infetar outros sistemas, primeiro precisa de pesquisar e encontrá-los. Isto é feito através de várias técnicas, tais como a digitalização de sistemas remotos (T1018), enumerando a sessão de desktop remoto ativa (T1563), a verificação de novas unidades anexas no sistema infetado (T1120). Uma vez encontrado um potencial dispositivo remoto ou unidade, o WannaCry tenta copiar-se para o sistema alvo e executa o seu comportamento malicioso.

Antes de o ransomware iniciar a sua encriptação, executa alterações no sistema infetado para desativar as opções de recuperação, que é referido pelo T1490. Em seguida, procura ficheiros específicos do utilizador em vários diretórios (T1083) e começa a encriptar cada ficheiro encontrado (T1486). Para a comunicação do servidor de comando e controlo, a rede Tor é utilizada (T1573/T1090).

Para uma identificação baseada no comportamento deste ataque, podem ser utilizadas as seguintes técnicas MITRE ATT&CK:

- ☑ T1210: Exploração de Serviços Remotos
- ☑ T1018: Descoberta do Sistema Remoto
- ☑ T1563: Sequestro de sessão de serviço remoto (.002 RDP Hijacking)
- ☑ T1120: Descoberta de dispositivo periférico
- ☑ T1490: Inibir a recuperação do sistema
- ☑ T1083: Descoberta de Arquivos e Diretórios
- ☑ T1486: Dados Encriptados para Impacto
- ☑ T1573: Canal criptografado (.002 Criptografia Assimétrica)

☑ T1090: Proxy (.003 Multi-hop Proxy)

RESPONDER

Já em 2017, um novo ransomware chamado WannaCry (WannaCrypt) que visa o sistema operativo Windows infetou milhares e milhares de clientes em todo o mundo. Em vez de visar uma organização específica, o ataque foi generalizado. Grandes empresas onde algumas delas estão a gerir os seus negócios em todo o mundo, como a fabricante de automóveis, foram atingidas pelo ransomware. No entanto, também outros grupos de organizações, como os transportes públicos, os serviços de saúde ou os serviços de telecomunicações, também foram afetados.

- ☑ **QUEM:** Desconhecido
- ☑ **A QUEM:** Diferentes empresas em todo o mundo
- ☑ **PORQUÊ:** Atingir altos danos devido à perda de dados e provavelmente ganhar dinheiro
- ☑ **O QUÊ:** Conhecimentos da empresa, tais como dados
- ☑ **COMO:** Infeção do ransomware que foi distribuída através de uma vulnerabilidade encontrada no Microsoft Windows
- ☑ **ESTRATÉGIA:** A nota de resgate utilizada pelo WannaCry apareceu no ecrã dos sistemas que estavam infetados. Sistemas antivírus e firewalls detetaram a infeção e a propagação do ransomware e, portanto, não impediram os sistemas de infeções e danos adicionais.

"O surto wannaCry, atingiu mais de 200.000 computadores em mais de 150 países. Custando ao Reino Unido 92 milhões de libras e aumentando os custos globais até 6 mil milhões de libras." (Acronis, 2020)

RECUPERAR

IMPACTO: As consequências deste ataque podem ser consideradas como perda de informação, uma vez que todos os ficheiros encriptados pelo ransomware já não são legíveis. Além disso, se as organizações tentaram pagar o resgate para recuperar os seus dados, também acabaram por ter um prejuízo financeiro.

ESTRATÉGIA DE RECUPERAÇÃO: O processo de recuperação de um ransomware pode demorar muito tempo. Todos os sistemas infetados devem ser reinstalados ou uma cópia de segurança tem de ser revertida. Se as cópias de segurança foram armazenadas num sistema infetado, obviamente não podem ser usadas para o processo de recuperação.

MELHOR ESTRATÉGIA

- ☑ Mantenha os sistemas antivírus atualizados
- ☑ Utilizar sistemas de deteção e prevenção de intrusões de intrusões
- ☑ Monitorizar adequadamente os sistemas para atividades suspeitas
- ☑ Configurar adequadamente sistemas e desativar os serviços não necessários
- ☑ Gestão de patch rápido para corrigir vulnerabilidades o mais rápido possível

- ☑ Conhecimento de formação dos colaboradores
- ☑ Utilize a segmentação a nível de rede e limite a comunicação permitida a um mínimo exigido

LIÇÕES APRENDIDAS

Os ataques de ransomware são hoje comuns e podem atingir todas as empresas. É altamente recomendado seguir práticas de segurança conhecidas para tornar a infraestrutura de TI o mais segura possível para limitar os danos de um ataque ao seu mínimo.

ESTUDO DE CASO 10: ESPIÃO EM DADOS PRIVADOS SENSÍVEIS

ORGANIZAÇÃO ALVO

No outono de 2020, a nível nacional foi anunciado um novo alerta de segurança. Especificou que muitas entidades públicas e privadas foram severamente afetadas, à semelhança de outras ondas sucessivas anteriores, por **ataques de malware do tipo EMOTET, o** que levou a inúmeros problemas. EMOTET é um **malware** que infeta computadores que executam o sistema operativo Microsoft Windows através de ligações ou anexos maliciosos infetados (por exemplo.PDF, DOC, ZIP, etc.).

COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação necessária para descrever este ciberataque foi recolhida através de uma entrevista com um técnico de TI da empresa. A interação foi realizada com a condição de manter informações sensíveis anonimamente. Mesmo que o entrevistado estivesse disposto a descrever o incidente, algumas informações não podiam ser obtidas porque o problema era delegado a uma empresa especializada e tinha de ser investigado separadamente.

PREVENIR

Embora tenham sido realizadas campanhas de sensibilização por entidades e organizações especializadas sobre as medidas a tomar, muitas organizações públicas e privadas foram afetadas, de acordo com os relatórios existentes.

No caso da empresa analisada, na perspetiva da cibersegurança, procedimentos e mecanismos específicos operados, mas estes não foram suficientes devido à baixa experiência no domínio digital de alguns trabalhadores.

"O EMOTET era muito mais do que apenas um malware. O que tornou o EMOTET tão perigoso é que o malware foi oferecido para aluguer a outros criminosos virtuais para instalar outros tipos de malware, como cavalos de troia bancários ou ransomware, no computador da vítima." (EUROPOL, 2022)

IDENTIFICAR

Emotet é um troiano inicialmente associado à fraude bancária que, desde 2017, se limitou a distribuição de spam e carga útil secundária. Atualmente pode ser identificado numerosas variantes do Emotet e infelizmente este malware continua a evoluir para novas variantes com capacidades mais complexas e técnicas de evasão.

Com base em descrições fornecidas e suplementos de relatórios mediáticos, os seguintes detalhes foram envolvidos na incidência:

☑ Um e-mail de phishing projetado socialmente foi recebido com um arquivo Zipped anexado e com a senha incluída na mensagem.

☑ Malware foi encriptado e protegido por palavra-passe num arquivo

☑ Soluções anti-malware evadidas usando arquivos protegidos por palavra-passe como anexos

☑ Ocarregador T rojan continha um código benigno de um Microsoft DLL para evitar soluções antivírus

☑ Thread hijacking para distribuir código malicioso usando arquivos protegidos por palavra-passe como anexos

☑ Sistemas comprometidos foram aproveitados para enviar e-mails maliciosos para outros contactos

☑ Sistemas de e-mail encerrados temporariamente para impedir a propagação de Troia

☑ Redes internas com impacto

De acordo com o modelo MITRE ATT&CK, esta incidência pode ser descrita da seguinte forma:

1. T1566.001 - Acessório de Spearphishing
2. T1204.002 - Execução do Utilizador: Ficheiro malicioso
3. T1027 - Ficheiros obfuscados ou informações
4. T1036 - Mascarar
5. T1586.002 – Contas de Compromisso: Contas de email
6. T1586.002 – Contas de Compromisso: Contas de email
7. T1499 - Endpoint Negação de Serviço
8. T1498 - Rede de Negação de Serviço

RESPONDER

QUEM: O agressor não foi identificado. Só o local de origem, o Vietname.
QUEM: alvo não específicado
PORQUÊ: Recolha de dados sensíveis e pagamentos de ransomware
O QUÊ: Dados da empresa/utilizadores
COMO: Anexo de spearphishing, execução de script, injeção de processo.

ESTRATÉGIA: A ameaça começou num computador sem antivírus e espalhou-se lateralmente. Um processo de limpeza foi realizado por uma empresa especializada em TI&C.

RECUPERAR

IMPACTO: As principais consequências do ataque foram como seguir:

- ☑ Perda de dados
- ☑ Perturbação regular da atividade
- ☑ Sistema comprometido
- ☑ Custos financeiros

Phishing é um termo abrangente para um tipo de ataques de engenharia social que são realizados atualmente através de e-mails ou aplicações de redes sociais.

ESTRATÉGIA DE RECUPERAÇÃO: A estratégia de recuperação centrou-se na limpeza e reinstalação dos computadores comprometidos, na limpeza e/ou na reinitialização das caixas de correio eletrónico de compromisso.

MELHOR ESTRATÉGIA

- ☑ Instale e mantenha um Antivírus/Antimalware atualizado
- ☑ Adotar uma prevenção de intrusão em rede
- ☑ Restringir conteúdo baseado na Web
- ☑ Assegurar a consciência do utilizador
- ☑ Melhores políticas de senha
- ☑ Gestão de Conta Privilegiada
- ☑ Desativar ou remover recurso ou programa
- ☑ Prevenção da Execução
- ☑ Auditoria
- ☑ Gestão de Conta de Utilizador
- ☑ Prevenção de Comportamento no Ponto Final
- ☑ Políticas de utilização de conta.

LIÇÕES APRENDIDAS

Mesmo que a Emotet tenha sido derrubada através de uma atividade concertada internacional, resta saber se isso terá um impacto de longa data.

Se é para notar que os malwares usam quase as mesmas técnicas para penetrar e espalhar na natureza, por isso é obrigatório Para tenha cuidado e cuidado, pois os ciberataques continuarão a existir no futuro. Medidas como considerar a comunicação com o mundo utilizando computador isolado da rede que acolhe infraestruturas críticas, utilizando soluções de segurança capazes e atualizadas, considerando ter atualizações mais recentes são algumas que devem ser previstas.

ESTUDO DE CASO 11: ACESSO ILÍCITO A CREDENCIAIS

ORGANIZAÇÃO ALVO

Como qualquer empresa moderna, no caso de uma situação descrita, as comunicações electrónicas através da Internet com os seus clientes e fornecedores são a forma mais preferencial. Neste tipo de comunicação, um dos mais utilizados é o e-mail eletrónico. Permite manter o contacto assíncronoso com as partes interessadas geridas de forma eficiente por mais do que uma pessoa. A empresa encontrada ao longo de meio século no mercado tem sido fortemente desenvolvida em digitalização em todos os departamentos, e neste contexto está incluída também o departamento de relações com clientes. Para colaboradores relacionados foi criado um grupo de e-mail para gerir os pedidos on-line de computadores dedicados protegidos pela funcionalidade de filtragem antivírus e spam no servidor de e-mail.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação necessária para descrever este ciberataque foi recolhida através de uma entrevista com um dos técnicos de TI da empresa. A interação foi realizada com a condição de manter informação sensível anonimamente. Mesmo que o entrevistado estivesse disposto a descrever o incidente, algumas informações não podiam ser obtidas porque o problema era gerido por uma equipa diferente.

PREVENIR

Embora tenham sido realizadas campanhas de sensibilização pela Direção Nacional de Segurança Cibernética sobre as medidas a tomar, muitos públicos, organizações privadas e indivíduos foram afetados, de acordo com os relatórios existentes.

A empresa impôs o uso de ferramentas de segurança e regulação personalizada sobre o trabalho online, mas estas não foram suficientes devido à experiência básica no domínio digital de alguns colaboradores.

IDENTIFICAR

Phishing denota um termo de guarda-chuva para um **tipo de ataques de engenharia social** que são realizados atualmente através de e-mails ou aplicações de redes sociais. Normalmente, os cibercriminosos enviam mensagens não solicitadas a granel. Querem atingir o maior número possível de pessoas, a fim de apanhar algumas delas com o seu truque.

Os cibercriminosos tentam explorar a tendência de algum tipo de "grandes ofertas" ou com algumas instruções administrativas. Muitos destes tipos de mensagens parecem ser legítimos, uma vez que utilizam a mesma identidade visual que empresas bem conhecidas, serviços online ou aplicações. Alguns exemplos incluem empresas como Google, Amazon, Microsoft, Yahoo, LinkedIn, etc. ou serviços e aplicações bancárias populares, como a gestão de e-mails baseados na Web.

A credibilidade pretende ser alcançada copiando o esquema de cores, estilo, logotipo e lema da identidade copiada. São utilizadas linhas típicas de assuntos atraentes.

Com base na descrição fornecida e relatórios suplementares dos meios de comunicação, os seguintes detalhes foram envolvidos na incidência:

- ☑ Foi recebido um e-mail de phishing projetado socialmente que alegava a necessidade de alterar urgentemente a palavra-passe de acesso para evitar o fim do serviço;
- ☑ A disponibilização de credenciais à entidade ilegítima levou ao acesso à conta de e-mail e à descontinuação do acesso legítimo por alteração de senha;
- ☑ A conta comprometida foi utilizada para mensagens de phishing não solicitadas enviadas para os contactos existentes e outros endereços pertencentes ao intruso;
- ☑ Devido às mensagens de correio publicitário não enviadas pela Internet, o serviço de correio eletrónico foi colocado na lista negra de tal forma que o funcionamento normal foi interrompido;
- ☑ O sistema de correio eletrónico foi suspenso temporariamente para impedir o envio de correio publicitário não solicitado;
- ☑ Houve impacto nas operações online.

De acordo com o modelo MITRE ATT&CK, esta incidência pode ser descrita da seguinte forma:

1. T1598.001 - Serviço de Spearphishing
2. Acessório T1598.002- Spearphishing
3. T1598.003- Ligação Spearphishing

RESPONDER

- ☑ **QUEM:** O agressor não pôde ser identificado com precisão, uma vez que, de vários países, foram registadas origens. Possível utilização da VPN esteve envolvido.
- ☑ **QUEM:** alvo não específico
- ☑ **PORQUÊ:** Recolha sensível de dados e extorsão de dinheiro
- ☑ **O QUÊ:** Dados da empresa/utilizadores
- ☑ **COMO:** Phishing, roubo de credenciais.
- ☑ **ESTRATÉGIA:** A ameaça começou por abrir um e-mail personificado, aceder a links falsificados e enviar dados sensíveis. A redefinição de credenciais e a deslistação dos serviços de blacklist foram realizadas pela equipa de TI.

RECUPERAR

IMPACTO: As principais consequências do ataque foram as seguintes:

- ☑ Perda de credencias
- ☑ Perturbação regular da atividade
- ☑ Sistema comprometido

ESTRATÉGIA DE RECUPERAÇÃO: A estratégia de recuperação foi focada em redefinir as credenciais e limpar os clientes de e-mail comprometidos.

MELHOR ESTRATÉGIA

- ☑ Instale e mantenha um sistema de filtragem Antivírus/Antimalware/Email atualizado
- ☑ Adotar uma prevenção de intrusão em rede
- ☑ Restringir conteúdo baseado na Web
- ☑ Assegurar a consciência do utilizador
- ☑ Melhores políticas de senha
- ☑ Gestão de Conta Privilegiada
- ☑ Auditoria
- ☑ Gestão de Conta de Utilizador
- ☑ Prevenção de Comportamento no Ponto Final
- ☑ Políticas de utilização de conta.

LIÇÕES APRENDIDAS

Mesmo que o phishing não seja uma nova técnica, continua a ser uma das principais formas de ataques de segurança cibernética.

Note-se que os malwares utilizam quase esta técnica para penetrar e espalhar-se na natureza, pelo que é obrigatório estar atento e cuidadoso, uma vez que os ciberataques desta forma continuarão a existir. Medidas como considerar a utilização de serviços de e-mail protegidos mais atualizados, uma maior sensibilização para o acesso a e-mails e uma análise adequada da legitimidade do remetente.

ESTUDO DE CASO 12: APLICAÇÕES DESATUALIZADAS EXPOSTAS

ORGANIZAÇÃO ALVO

Hoje em dia, muitas empresas mudaram a forma de prestar os seus serviços movendo-se online. É o caso do exemplo desativado, em que, na mesa de serviços de tipo financeiro iniciado em 1998, foram migrados online durante mais de uma década. A nova abordagem melhorou a atividade global da empresa e a satisfação dos clientes. No entanto, estas realizações só foram possíveis após um esforço importante no desenvolvimento do necessário software personalizado desenvolvido internamente. Esta aplicação online permitiu que os clientes e os colaboradores realizassem as operações necessárias. A plataforma fornecida desenvolveu-se nessa altura até que o suporte estava disponível antes do lançamento da nova grande atualização. Com o tempo, o número de colaboradores foi reduzido devido aos processos existentes de automação e mudanças de mercado. A atualização para a nova distribuição foi adiada, uma vez que foram necessários grandes hardware e software.

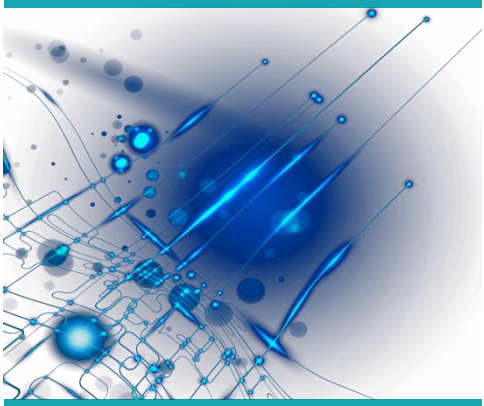
COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação necessária para descrever este ciberataque foi recolhida através de uma entrevista com o CEO da empresa. A interação foi realizada com a condição de manter informações sensíveis anonimamente.

PREVENIR

Embora tenham sido levadas a cabo campanhas de sensibilização pela Direção Nacional de CiberSegurança sobre as medidas a tomar, muitos públicos ou organizações privadas ignoram ou atrasam a decisão e as ações necessárias para atualizar os seus sistemas de informação.

A empresa impôs o uso de soluções de segurança conhecidas, firewalls, segmentação de rede, etc. mas estas não foram suficientes, uma vez que permaneceu a vulnerabilidade exposta num dos módulos de software operados.



IDENTIFICAR

Os ataques de injeção de fluxo abusam da capacidade de uma aplicação web online aceitar conteúdo carregado, como diferente tipo de documento ou ficheiros de imagens. Utilizando uma abordagem de inclusão de ficheiros remotos, um intruso pode explorar a vulnerabilidade no código do lado do servidor para aceitar um URL em outro site como uma entrada válida. Esta ação é então usada para executar código de agressor malicioso. Adicionalmente, a inclusão de ficheiros locais pode ser usada para obter uma aplicação web para devolver o conteúdo desejado do sistema de ficheiros local.

Um exemplo popular é recebido no caso da estrutura PHP utilizada pelo WordPress permitindo ao hacker aceder ao seu ficheiro de configuração. Este ataque também pode permitir o acesso ao download de quaisquer ficheiros de códigos de código PHP que executam o website, oferecendo novas possibilidades para outras vulnerabilidades de segurança. Versões phP recentes estão protegidas contra a inclusão remota de ficheiros por padrão, mas se por engano a inclusão de ficheiros locais é exposta este tipo de ataque ainda é possível.

Com base na descrição fornecida, relatórios técnicos suplementares, boletins de segurança e vulnerabilidades, os seguintes detalhes foram envolvidos no incidente:

- ☑ Por um ataque tipo força bruta, uma conta protegida com uma senha fraca é acesso ilegítimo;
- ☑ As credenciais descobertas permitem alterar os dados associados à conta;

- ☑ A conta comprometida permitiu que a vulnerabilidade da injeção de fluxo fosse exposta e a execução de código indesejada no servidor foi usada para remover os registos do histórico de acesso;
- ☑ Devido à execução de código lateral do servidor descontrolado, alguns módulos da aplicação tornam-se inutilizáveis e conduzem ao encerramento do serviço para que o funcionamento normal tenha sido interrompido;
- ☑ O sistema foi desligado temporariamente da Internet para uma investigação mais aprofundada relacionada com o mau funcionamento da aplicação web;
- ☑ Houve impacto nas operações online.

De acordo com o modelo MITRE ATT&CK, esta incidência pode ser descrita da seguinte forma:

1. T1110.001 - Adivinhar da palavra-passe
2. T1078 - Acesso válida a contas
3. T1518 - Descoberta de Software
4. T1082 - Descoberta de Informação do Sistema
5. T1007 - Descoberta do Serviço de Sistema
6. T0826 - Perda de Disponibilidade.

RESPONDER

- ☑ **QUEM:** O agressor não pode ser identificado com precisão.
- ☑ **A QUEM:** alvo não específicado
- ☑ **PORQUÊ:** Recolha sensível de dados e negação de serviço
- ☑ **O QUÊ:** Dados da empresa/utilizadores
- ☑ **COMO:** Ataque à força bruta, roubo de credenciais e execução de código por injeção de fluxo.
- ☑ **ESTRATÉGIA:** A ameaça começou por um ataque de força bruta que levou a uma fraca descoberta credencial, explorando a vulnerabilidade num módulo de software acessível não público e, em seguida, a execução não autorizada de código. A fraca estratégia de proteção de acesso online, módulo de software desatualizado e código não mantido são a principal causa da incidência.

RECUPERAR

IMPACTO: As principais consequências do ataque foram:

- ☑ Perda de credenciais
- ☑ Sistema comprometido
- ☑ Perturbação regular da atividade.

ESTRATÉGIA DE RECUPERAÇÃO: A estratégia de recuperação foi focada na reescrita da plataforma principal, reescrevendo uma parte importante do código.

MELHOR ESTRATÉGIA

- ☑ Instale e mantenha um software atualizado
- ☑ Impor uma política de senhas fortes
- ☑ Políticas de utilização de conta

- ☑ Adotar mecanismo de autenticação de dois fatores
- ☑ Adotar uma prevenção de intrusão em rede
- ☑ Restringir o acesso remoto
- ☑ Assegurar a consciência do utilizador
- ☑ Implementar uma auditoria periódica de segurança
- ☑ Gestão de Conta de Utilizador
- ☑ Prevenção de Comportamento no Ponto Final.

LIÇÕES APRENDIDAS

Mesmo que se saiba que o software de execução desatualizado é propenso a vulnerabilidades de segurança, continua a ser uma das principais formas de muitos ataques de segurança cibernética.

Aplicações web acessíveis em todo o mundo estão expostas a muitas vulnerabilidades e, como consequência, requerem uma atenção especial de muitas perspetivas.

Medidas como considerar a atualização constante de software, melhorias e adoção de novas técnicas e solução para mecanismos de autenticação, a adoção de um processo de auditoria de base regular são algumas das medidas comuns que podem ser consideradas.

ESTUDO DE CASO 13: OS RISCOS DE UM ATAQUE FEITO POR UM EX-FUNCIONÁRIO

ORGANIZAÇÃO ALVO

A organização onde ocorreu o ciberataque, atua no acompanhamento comercial, numa sucursal automóvel, com cerca de 2000 funcionários. Localizado no estado do Paraná e Santa Catarina no Brasil.

O ciberataque visou a área das tecnologias da informação, devido ao conhecimento que o hacker tinha de ser um ex-funcionário da organização, dando-lhe o benefício de convencer o sistema.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação aqui apresentada baseia-se num estudo de caso sobre os riscos de um ciberataque liderado por um ex-funcionário. O estudo de caso é feito do ponto de vista da organização que sofreu o ciberataque.

O objetivo geral deste estudo de caso é demonstrar a importância que as empresas devem pagar em relação à engenharia social nos seus ambientes, a fim de evitar invasões e/ou fraudes causadas pela imprudência ou assistência não intencional dos colaboradores como violações ao trabalho do hacker.

PREVENIR

Para evitar possíveis danos, a empresa já possuía um departamento de TI que geria firewalls, ferramentas de fuga de informação e encriptação de dados.

IDENTIFICAR

Neste estudo de caso, o footprint começou com várias visitas à página da associação, com a intenção de compreender a sua dinâmica, os seus negócios e especialmente as suas marcas (considerando que o agressor dirigiu a procura de dados que o hacker ainda não conhecia). Quando a pegada começou e a informação interna e específica da organização está do lado do atacante, ele passou a fazer ligações a uma das lojas da cadeia para descobrir os nomes dos gestores e pessoas que poderiam ter acesso privilegiado dentro da organização.

Para tal, o agressor posou, por telefone, como um cliente que tinha problemas legais com a empresa. Para resolver este problema, a empresa teria chamado o cliente e pedido-lhe para falar com o gerente da loja em questão, uma vez que seria a pessoa com maior autonomia para responder a tal situação. Devido a esta interação, foi facilmente alcançado, o nome do gerente, o local de onde trabalhava e o número de telefone.

Após este telefonema, foram feitas tentativas de contactar o gestor nos canais informados para verificar as informações recolhidas. O reset da palavra-passe foi feito quando contactado com o sector das tecnologias da informação, fazendo-se passar pelo próprio trabalhador, de forma a obter esse setor mencionado para o informar dos dados de acesso do utilizador.

Usando um pouco de persuasão, e o argumento de que os dados para o conselho dependiam deste acesso, finalmente o técnico repôs a senha e informou a nova senha por telefone. Mais do que isso, foi possível convencê-lo a estabelecer acesso VPN (tecnologia para acesso remoto ao ambiente da empresa) para que o utilizador hipotético poderia trabalhar de fora do escritório.

RESPONDER

QUEM: The attacker was an ex-employee;
A QUEM: Uma organização que trabalha no acompanhamento comercial, na filial automóvel;
PORQUÊ: O ataque foi dirigido à organização com motivos desconhecidos;
O QUÊ: A propriedade visada foi o setor das tecnologias da informação, a fim de recolher informação privilegiada da organização e dados pessoais dos atuais colaboradores;

COMO: O ataque começou com a obtenção do nome do gerente de uma loja, procedeu a contato com o setor de tecnologias de informação da empresa e convinc ed-los para redefinir a senha. Dessa forma, o ex-funcionário fingia ser o gerente e tinha acesso a tudo o que diz respeito a informação privilegiada, dados pessoais de funcionários e clientes e tudo o mais que o hacker quisesse.

RECUPERAR

A empresa começou a formar os colaboradores para prestar atenção aos tipos de informação que normalmente transmitem a terceiros, especialmente se forem informações críticas. Nunca, em nenhuma circunstância, um funcionário deve passar informações críticas, como palavras-passe, por telefone. Estas devem ser fornecidas às partes interessadas através de métodos seguros, tais como cartas registadas ou através do gestor responsável.

Também forneça formação para sensibilizar os colaboradores para o cuidado com a informação que partilham na internet. A formação centrou-se nos riscos que a informação partilhada pode trazer à sua ocupação, mas também trazer à vida pessoal, tais como raptos, detalhes da vida e segurança pessoal.

Esta empresa está consciente de que precisa de proporcionar condições técnicas e físicas para a aplicação de boas práticas de segurança, mas, acima de tudo, valorizar e incentivar a adoção de boas práticas e protocolos de segurança mais rigorosos pelos seus colaboradores, seja num ambiente corporativo ou pessoal, a fim de controlar, da melhor forma possível, o fator mais fraco de segurança da informação: o fator humano.

LIÇÕES APRENDIDAS

A organização deve estabelecer a informação num procedimento simples que possa frustrar o hacker. Este procedimento tem 3 etapas:

☑ **Público:** Informação que poderia ser dada a qualquer pessoa, por exemplo, a contactos comerciais e empresas específicas, informação entre clientes e negócios da empresa;

- ☑ **Privado:** Informação que não pode ser dada a qualquer pessoa e que apenas diz respeito ao ambiente corporativo. São abrangidas por esta categoria informações referentes a procedimentos internos, dados corporativos administrativos e aspetos estratégicos da empresa;
- ☑ **Confidencial:** Informações e dados que não devem ser partilhados dentro e fora da empresa, tais como dados de registo de trabalhadores, compensações, resultados de sectores e ações estratégicas que apenas dizem respeito à direção ou presidência.

Além disso, as organizações devem ter procedimentos internos para protegê-los de ataques de engenharia social. Os operadores devem estar bem treinados sobre os processos que devem seguir e as ações que devem tomar em situações em que a empresa se sinta atacada, como a transferência da chamada para uma pessoa treinada para lidar com este tipo de situação. Ações simples podem fazer com que o ataque falhe. Imediatamente pode dizer-se que uma primeira lista de verificação para confirmar os dados do requerente já iria dificultar o acesso do hacker. Tendo em conta que os dados pessoais não são algo muito difícil de obter, os técnicos poderiam adotar um processo de devolução do contacto ao número de telefone registado do colaborador, de forma a confirmar que se trata, de facto, do trabalhador em causa.

ESTUDO DE CASO 14: CIBERATAQUES COMO UM NOVO DESAFIO DE SEGURANÇA INTERNA

ORGANIZAÇÃO ALVO

Entidades governamentais portuguesas (especialmente o Ministério da Administração Interna), as Forças de Segurança e as grandes empresas.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação para este estudo de caso foi recolhida através de uma investigação referente a uma tese de mestrado, onde o autor aplica um estudo e várias entrevistas exploratórias com especialistas e pessoas responsáveis pelas forças de segurança nacionais, a fim de concluir se o fenómeno hacktista representa uma ameaça para as forças de segurança portuguesas.

PREVENIR

Para prevenir ataques, uma das medidas que a equipa de TI responsável pela cibersegurança nestas organizações toma é monitorizar os canais sociais, por exemplo: IRC's (Internet Relay Chat), todo o tipo de conversas, Facebooks, tudo a partir do qual é possível obter informações na internet, eles também fazem um acompanhamento e tentam ver se há alguma ação suspeita.

De acordo com o "modus operandi", definido pelos termos do grupo Anonymous (Portugal), inicialmente publicitam nas redes sociais (IRC's e Facebooks), as ações que vão tomar e é aí que começam a comunicar entre eles. Depois usam canais de chat privados para comunicar uns com os outros, o que levou à implementação do SOC (Centro de Operações de Segurança) do MIA (Ministério da Administração Interna), para se prepararem para este tipo de ataques.

IDENTIFICAR

As consequências destes ataques variaram, dependendo do tipo de ataque. Muitos lidaram com um ataque de negação de serviço, (DOS, DDOS), que provoca um esgotamento de recursos em termos de sistemas ou comunicações. Além disso, lidaram com alguns tipos de tentativas de ataques de intrusão, como injeção de SQL e desfigurações. Pesca por e-mail, é também um dos ataques mais frequentes, levando às vezes ao acesso à informação privada.

Em novembro de 2011, foi realizado um ataque no site do sindicato nacional para a carreira dos Chefes de Equipa da PSP, com a divulgação de dados pessoais e confidenciais (patentes, números de telefone e endereços de correio eletrónico) de 107 efetivos da PSP..

"Os ataques de DDoS têm vindo a aumentar de frequência nos últimos anos. De acordo com um relatório da Cloudflare, os ataques do Resgate DDoS aumentaram quase um terço entre 2020 e 2021 e aumentaram 75% no 4º trimestre de 2021 em comparação com os três meses anteriores.". (Cook, 2022)

RESPONDER

Um ataque à Polícia de Segurança Pública foi assumido pelo grupo LulzSec Portugal. O grupo Português Anónimo tem reivindicado vários ataques a sites governamentais e instituições relevantes. Geralmente, o perfil do hacker é de alguém jovem, em idade escolar, no nível secundário (10º ao 12º ano). Pode haver uma ou outra situação em que já são mais pessoas adultas, talvez com menos conhecimento na área tecnológica, mas insatisfeitas com a sociedade.

Este tipo de ataque está disponível para qualquer cidadão. Basta levar a pessoa a procurar na internet ferramentas, métodos e grupos e começar a participar. Estes grupos de pessoas anónimas, na altura dos ataques, realizaram workshops sobre como fazer um ataque, cursos "abc" sobre como entender o ataque. Eles fornecem ferramentas já desenvolvidas e que qualquer pessoa pode aceder ao site, só é necessário inserir o endereço de destino e uma aplicação desenvolve o ataque.

A maioria dos agressores, ou seja, os jovens ainda na escola, usam ferramentas que são usadas por muitos especialistas, esses especialistas são pessoas com um grau académico mais avançado, e mais velhos, que usam ferramentas já desenvolvidas para fins de ciberataque. Ou seja, na internet, é possível pesquisar e obter informações para realizar o ataque, como fazê-lo e que tipo de ferramentas são usadas para ajudar a fazer o ataque.

O ataque feito pela LulzSec Portugal foi justificado no Twitter alegando que como resposta à ação dos agentes provocadores infiltrados numa manifestação organizada por eles.

Mas na maior parte do tempo estes ataques acontecem porque estas pessoas procuram visibilidade ou para comprometer as organizações, como isso muitas vezes tem a ver com o descontentamento das pessoas em termos do contexto atual em que os cidadãos portugueses vivem, e muitas vezes as pessoas demonstram o seu desagrado desta forma. Outras vezes é apenas uma piada para os agressores, com idades compreendidas entre os 16 e os 17 anos, que não têm muitas preocupações em termos sociais, é muitas vezes porque os amigos o fazem, e para se promoverem dentro do grupo de amigos, outras vezes são experiências que fazem porque é a idade de experimentar coisas novas. A maior parte do tempo não percebem o impacto que estes ataques podem ter.

Tudo começa com um grupo de hackers que têm o conhecimento técnico e desenvolvem ferramentas para serem usados por grupos de pessoas que não têm o mesmo conhecimento, o que torna o processo de hacking fácil para qualquer pessoa.

Uma característica dos grupos portugueses é atacar sites desprotegidos e explorar vulnerabilidades. Planeiam ataques ao IRC's (Internet Relay Chat) e salas de chat, não assumem a sua identidade e usam apelidos. Os hacktivistas portugueses usam as ferramentas disponíveis online para realizar os ataques, ou seja, "não fabricam programas personalizados, mas utilizam os que estão disponíveis na rede". Quanto às pessoas que assumem a organização e liderança deste tipo de iniciativa, são muitas vezes pessoas com pouca experiência técnica, dedicando-se a fazer anúncios e a divulgar as ações a desenvolver, e muitas vezes "aqueles que até têm competências técnicas muito especializadas, não fazem ideia de que são os mais competentes e especializados no grupo, pensam que são pessoas que pouco sabem e que estão apenas a ajudar os outros que sabem mais".

O grupo Anonymous utiliza métodos de hacking convencionais como Havij114 e SQL Injection, sendo a sua principal inovação a criação de websites que realizam ataques DoS.

RECUPERAR

As possíveis consequências são o roubo de informação, a indisponibilidade dos serviços e os desacabamentos nos sites onde são feitas alterações na informação, uma vez que os hackers por vezes removem informações, também podem adicioná-la.

Estes ataques podem comprometer a confiança depositada pelos cidadãos nas instituições que são vítimas destes grupos, mas também a identificação de vulnerabilidades e a influência de outras pessoas com determinados ideais são situações que podem acontecer.

Este tipo de ataques evoluem, e as técnicas melhoram ao longo do tempo, e as organizações devem ajustar-se e evoluir para a proteção da sua rede. Foram obrigados a deixar de aceder à rede até que as condições fossem satisfeitas para garantir a manutenção da segurança da informação interna. E já

o fizeram, no total, durante uma hora, no máximo. Ocasionalmente, alguns serviços também têm sido inacessíveis durante a noite.

O CNCseg (Centro Nacional de Cibersegurança) está a ser desenvolvido, o que terá mais a ver com a questão da defesa nacional, do que com o Centro de Defesa Cibernética, que é da competência do Ministério da Defesa Nacional, cuja principal ação é o ataque a hackers que possam estar a desenvolver ataques, fazendo a deteção e contra-ataque destes elementos.

O MIA participará, pelo menos no CNCseg, que está a trabalhar em conjunto com o GNS, que é a entidade que tem essa competência e será um dos inputs de informação para este tipo de cibersegurança, a ideia é que este centro tenha a informação sobre o que está a acontecer a nível nacional, o objetivo é recolher informação tanto dos centros tecnológicos da Administração Pública, banca, indústria, as várias áreas da sociedade portuguesa e, com isso, têm uma ideia do impacto e do âmbito que podem ter um certo tipo de ataque.

LIÇÕES APRENDIDAS

O hacktivismo é visto como um novo desafio para as instituições e, especialmente, no caso das Forças de Segurança, um ataque hacktivista pode causar consequências nefastas, que podem até influenciar o desempenho das suas missões, sendo por isso considerado uma ameaça real, no sentido em que isso se caracteriza por contradizer os objetivos da organização, produzindo, em regra, danos materiais e/ou morais.

A capacidade dos grupos hacktivistas de realizar um ataque é geralmente baixa, uma vez que utilizam ferramentas disponíveis na rede e não são muito inovadoras em termos de hacking, aproveitando a exploração de vulnerabilidades existentes. No que diz respeito à oportunidade, qualquer pessoa de um computador com acesso à rede e com algum conhecimento ou vontade de aprender com a informação disponível na rede é capaz de desenvolver um ciberataque, e este facto torna-se preocupante para as forças de segurança.

Em termos de segurança informática, costuma-se dizer que não existe segurança total e que não existem sistemas 100% seguros, pelo que o governo e Portugal não são uma exceção. O que tem sido testemunhado é a criação de um conjunto de infraestruturas que permitam uma estrutura de segurança que possa corresponder e responder a este tipo de fenómeno: o recém-criado CNCseg, feito pela PJ para combater o cibercrime. Educar as pessoas é certamente algo que irá desafiar todos a perceber que também usamos novas tecnologias, plataformas de internet e outras redes que têm o poder de mudar a segurança dos seus cidadãos.

As consequências de um ataque hacker às forças de segurança nacional:

- ☑ Direto: consequências económicas, sociais, políticas e de segurança.

☑ Indireta: o sentimento de segurança, desregulamentação social e, em última análise, a soberania do país, das instituições e das famílias.

ESTUDO DE CASO 15: A "IDADE DE OURO" DO "RANSOMWARE". COMO PREVENIR E LIDAR COM UM SEQUESTRO DE DADOS

ORGANIZAÇÃO ALVO

A maioria das empresas portuguesas está na "geração 3" de cibersegurança e os ataques estão na "geração 6". Neste estudo de caso aprendemos sobre como proceder para prevenir ataques de ransomware como o que o grupo IMPRESA enfrenta, cada vez mais frequentemente.

IMPRESA is the largest portuguese media group, operating in three business areas — print, digital and television.

"O ransomware vai custar às vítimas mais de 265 mil milhões de dólares por ano até 2031." (Cybersecurity Ventures).

COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação para este estudo de caso foi adquirida através de uma notícia sobre a prevenção de ransomwares, que inclui a entrevista de Rui Duro, especialista em cibersegurança..

PREVENIR

Os tempos de pandemia facilitaram o crescimento deste tipo de ataque de ransomware. Por um lado, trabalhar em casa, o que leva à dispersão de sistemas e aumenta o risco. Por outro lado, cada vez mais aplicações são sistemas migratórios para a "nuvem".

"Isto tem vários riscos associados", diz Rui Duro. Os sistemas estão agora "noutro prestador de serviços" e é necessário "comprar tecnologia também para a nuvem porque não é seguro em si mesmo". Para o especialista, "esta evolução para a 'nuvem' foi muitas vezes mais rápida do que a evolução do conhecimento dos colaboradores das tecnologias da informação".

Por outro lado, muitas empresas foram ultrapassadas pela sofisticação dos ataques. "Nós (grupo IMPRESA) estamos na geração 6 de ataques e a maioria das empresas ainda está na geração 3, numa fase muito inicial de proteção dada a evolução dos ataques. A mentalidade tem de mudar, tem de haver um orçamento, e recursos para se adaptar a esta nova realidade", explica Rui Duro.

IDENTIFICAR

Nas páginas dos sites do grupo, surge uma mensagem semelhante à que a SIC (canal de televisão português) recebeu: "Os dados internos dos sistemas foram

copiados e apagados. 50 TB de dados está nas nossas mãos. Contacte-nos se quiser os dados de volta".

Rui Duro explica que "normalmente surge o ransomware nas empresas através daquilo a que chamamos a colocação de uma 'carga útil' inicial dentro da empresa".

Isto acontece de diferentes formas, como através de um ataque de phishing a um elemento da empresa. Outras vezes, alguém na empresa "descarrega" inadvertidamente o malware. Há ainda uma terceira via, quando os atores têm o propósito de atacar uma empresa específica e estão à procura de vulnerabilidades - trata-se de um "ataque alvo".

Depois de o malware inicial estar dentro da empresa, este descarrega um segundo malware, que realiza o ransomware. Em seguida, começa a fazer uma "digitalização", procurando servidores e outros sistemas. O objetivo é obter o máximo de lucro possível - segundo o especialista, para os criminosos "não faz sentido encriptar um ou dois computadores, a ideia é encriptar o maior número possível de computadores, e de preferência os vitais".

Os hackers instalam então o malware no maior número possível de sistemas, mas não encriptam os dados de imediato. Normalmente, "fica por várias semanas, às vezes mais tempo".

Aqueles que atacam sabem que uma das formas de recuperação das empresas é através de backups - por isso esperam que haja um backup, e assim que é restaurado, há uma infeção novamente.

Quando a encriptação ocorre, os criminosos pressionam as empresas, normalmente para pedir um resgate em dinheiro – normalmente em criptomoedas.

RESPONDER

Dois dias depois de o grupo de hacking "Lapsus$ Group" ter atacado os sites do grupo Impresa, os sites ainda estavam indisponíveis.

A Polícia Judiciária Portuguesa confirmou que está a investigar o caso, juntamente com o Centro Nacional de Cibersegurança (CNCS), como o grupo de media já tinha avançado.

Este atraso na reposição de sistemas é comum em ataques como este. Segundo Rui Duro, responsável pela Check Point Software em Portugal, "o tempo necessário para lidar com estes ataques varia muito. Depende muito da dimensão da empresa, do ataque, da capacidade da empresa em termos de tecnologias de informação (TI) e da preparação da empresa para substituir os sistemas. Numa pequena empresa, às vezes demora um ou dois dias, se é uma grande empresa, pode até levar várias semanas e às vezes pode implicar refazer toda uma infraestrutura".

O ataque de ransomware já se tornou uma ameaça real e próxima a empresas de todo o mundo - e Portugal não é exceção. Para a Agência Europeia de Cibersegurança (ENISA), a pandemia trouxe consigo uma "idade de ouro" para os cibercriminosos.

De acordo com a agência, entre abril de 2020 e julho de 2021, houve um aumento de 150% nos ataques registados.

Em Portugal, ainda não existem dados oficiais sobre o último ano, mas no relatório anual de segurança interna, para 2020, o ransomware já está identificado como "a forma mais comum de sabotagem informática, tendo mantido elevadas taxas de casos e afetando especialmente as instituições do governo e das pequenas e médias empresas".

De acordo com este relatório, os ciberataques duplicaram em Portugal de 2019 (754 incidentes) para 2020 (1418 incidentes). Na área da Segurança da Informação, onde os ataques de ransomware são predominantes, em 2020 houve cerca de 10 vezes mais incidentes do que em 2019. Rui Duro, responsável pela Check Point Software em Portugal, explica que "90 a 95% dos casos não são reportados ou conhecidos. As empresas acabam por recuperar através de backups e não reportam ataques".

De acordo com os dados de um estudo divulgado pela empresa que dirige, que cria soluções de segurança tecnológica para as maiores empresas do mundo, as organizações portuguesas sofrem uma média de 947 ataques de malware por semana, um número superior à média global de 870 ataques. Cerca de 90% dos ficheiros maliciosos chegam por e-mail.

Os dados do Check Point Software mostram também que, em dezembro de 2021, os ataques de ransomware atingiram mais de 2,5% das empresas portuguesas.

RECUPERAR

Um ransomware é uma forma de malware (combinação das palavras inglesas "malicioso" e "software") projetado para encriptar servidores e áreas de armazenamento de computador.

Normalmente, os "hackers" por detrás das mensagens de exibição de ataque exigem o pagamento de uma quantia para desencriptar o sistema e devolvê-lo ao proprietário. De acordo com o especialista em cibersegurança, os ataques de ransomware são cada vez mais sofisticados e os piratas são cada vez mais vistos a tentar "duplicar ou triplicar a extorsão".

Em dupla extorsão, "durante o período em que o malware está à espera de cópias de segurança, copiam dados significativos de bases de dados, servidores de e-mail, servidores financeiros, tentam procurar dados sensíveis e exportam enormes quantidades de dados. E dizem que não vale a pena tentar recuperar o serviço com backups, porque têm os dados reféns".

No caso da tripla extorsão, com os dados sensíveis na sua posse, os piratas ameaçam visar os clientes e fornecedores da empresa se a empresa não pagar o resgate.

LIÇÕES APRENDIDAS

Para evitar um ataque é necessário mudar mentalidades e assumir que vai acontecer. Para o especialista em cibersegurança, isto é o mais importante. "Tenho mais de 30 anos no mercado a trabalhar nesta área, comecei quando os ataques foram uma piada, comparado com o que são hoje, mas ainda hoje vejo os decisores a pensar que ainda não é preocupante, não é relevante e que acham que não lhes vai acontecer. O primeiro passo é mudar essa mentalidade. Pode acontecer a todos, há pouco tempo aconteceu com a EDP. Quando acontecer, tenho de estar preparado para isso".

Leve a sério os três pilares da cibersegurança: pessoas, processos e tecnologia

a) Pessoas

"Muitas vezes, mesmo as empresas que levam a sério a cibersegurança focam-se demasiado na tecnologia como forma de se protegerem e esquecerem que é necessário formar pessoas para se comportarem com segurança", diz o especialista.

b) Processos

"É importante ter um processo para recuperar do desastre, gerir e qualificar informação, ter um processo de backup eficaz, ter repositórios de informação. Muitas empresas não estão preparadas, e as primeiras horas são um caos completo, porque não tiveram o cuidado de preparar o processo para recuperar", revela..

c) Tecnologia

"Usando tecnologia adequada à realidade que temos hoje. Muitas empresas compram tecnologia e é o que eu chamo de comprar uma "falsa sensação de segurança" - compram tecnologia, mas já não é adequada para a realidade que temos hoje. a firewall tradicional, em vez de comprar um ponto final avançado que evita a encriptação dos sistemas, é usado um ponto final simples, que deteta algum malware mas não impede estas encriptações".

O especialista lembra que, nestes casos, "o pânico não ajuda em nada". Nestas situações, é necessário informar as autoridades e nunca pagar o resgate, pois é o mesmo que perpetuar o crime, dizendo aos criminosos que vale a pena. Um dos processos que as empresas devem ter antecipadamente, para o especialista, é como recuperar de tal ataque, para que possa haver essa calma e para que todos saibam o seu papel neste processo.

ESTUDO DE CASO 16: MALWARE/ KEYLOGGER

ORGANIZAÇÃO ALVO

Uma pequena empresa de fabrico familiar fez uso extensivo da banca online. O funcionário contabilístico iniciou sessão no sistema bancário online com uma empresa e um ID e senha específicos do utilizador. Duas questões de desafio tiveram de ser respondidas para transações superiores a €1.000.

O proprietário foi notificado de que foi iniciada uma transferência de 5.000 euros por uma fonte desconhecida. Contactaram o banco e identificaram que em apenas uma semana os cibercriminosos tinham feito dez transferências das contas bancárias da empresa, num total de 10 mil euros. Como é que é? Um dos seus empregados tinha aberto um e-mail a partir do que pensavam ser um fornecedor de materiais, mas era, em vez disso, um e-mail malicioso ligado a malware de uma conta de impostor.

Os atacantes conseguiram instalar malware nos computadores da empresa, utilizando um keylogger para capturar as credenciais bancárias. Um keylogger é um software que monitoriza silenciosamente as teclas do computador e envia a informação para um ciber-criminoso. Podem então aceder online a serviços bancários e outros serviços financeiros, utilizando números de conta válidos e senhas.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação para este ciberataque foi recolhida através de duas entrevistas, uma com o proprietário da empresa e outra com um técnico da empresa de suporte informático. Ambos estavam dispostos a descrever e dar detalhes do incidente, mas pediram para manter as duas empresas anónimas porque a informação era demasiado sensível para eles.

Um keylogger é um software que monitoriza silenciosamente as teclas do computador e envia a informação para um ciber-criminoso.

PREVENIR

Na empresa analisada, os procedimentos e mecanismos de cibersegurança foram identificados como não satisfatórios. Embora os computadores da empresa tivessem software antivírus, ninguém foi atualizado. Além disso, não foram realizadas campanhas de sensibilização e alguns funcionários parecem ter uma compreensão limitada dos ciber riscos.

IDENTIFICAR

Com base nas informações fornecidas, foram recolhidos os seguintes detalhes sobre a incidência:

☑ Um e-mail de phishing projetado socialmente foi recebido com um arquivo com fecho comprimido anexado como verificação a uma ordem de fornecedor.
☑ Ao abrir o ficheiro, o malware foi instalado no computador.
☑ Um software keylogger foi instalado e monitoriza silenciosamente as teclas do computador e envia a informação para um ciber-criminoso.
☑ Em seguida, o ciber-criminoso usa as credenciais capturadas para aceder à conta bancária e fez a transferência usando números de conta válidos e senhas.
☑ O incidente só foi identificado quando o cibercrime tenta fazer uma transferência superior a 1000 euros.

RESPONDER

Não tendo um plano de cibersegurança no lugar, a resposta da empresa ao ataque foi adiada.

QUEM: The attacker could not be precisely identified. Only an email address was known and the possible origin.
A QUEM: Alvo não especificado
PORQUÊ: Recolha de dados sensíveis e utilização de dados para roubar dinheiro
O QUÊ: Credenciais de conta bancária da empresa

COMO: Keylogger, monitoriza silenciosamente as teclas do computador

ESTRATÉGIA: A ameaça começou num computador sem antivírus. Um processo de limpeza foi realizado por um perito em TIC de uma empresa. A conta bancária fechou e as credenciais mudaram. A empresa de TIC ajudou-os a completar uma revisão completa da cibersegurança dos seus sistemas e a identificar qual foi a origem do incidente. Também recomendam upgrades para o seu software de segurança.

RECUPERAR

IMPACTO: A empresa fechou a sua conta bancária e prosseguiu com uma ação judicial para recuperar os seus prejuízos. O negócio recuperou uma pequena parte dos prejuízos. Não há dinheiro para o tempo e as taxas legais foram recuperadas.

RECUPERAR: A estratégia de recuperação centrou-se no encerramento da conta bancária para evitar mais perdas. Outras ações foram, limpeza do computador e da caixa de correio eletronica comprometidos. Verifique todos os computadores da empresa para qualquer outro ataque.

ESTRATÉGIA: A empresa deve implementar várias ações para prevenir tais incidentes. A sua estratégia deve concentrar-se nas seguintes ações/passos:

- ☑ Implementar políticas de segurança como alterar a política de palavras-passe e a política de gestão de utilizadores de conta.
- ☑ Instale e mantenha um software Antivírus/Antimalware atualizado.
- ☑ Realizar programas de formação para assegurar a consciencialização dos colaboradores.
- ☑ Restringir o conteúdo baseado na Web.
- ☑ Efetue verificações e auditorias regulares.
- ☑ Executar Prevenção e implementação de um sistema de gestão de riscos.

LIÇÕES APRENDIDAS

- ☑ Notificações - criar alertas de transações em todos os créditos, cartões de débito e contas bancárias.
- ☑ Controlo de acesso. Restringir o acesso a contas sensíveis apenas aos funcionários que necessitem de acesso; mudar palavras-passe mais vezes.
- ☑ A empresa deve avaliar o seu risco e avaliar as opções de seguro de responsabilidade cibernética.
- ☑ Escolha bancos que ofereçam várias camadas de autenticação para aceder a contas e transações.
- ☑ Criar, manter e praticar um plano de resposta a incidentes cibernéticos que seja rapidamente implementável.
- ☑ Os cibercriminosos entregam e instalam software malicioso via e-mail. Treine funcionários na segurança de e-mail.

ESTUDO DE CASO 17: UM COMPUTADOR ROUBADO CAUSA UMA GRAVE VIOLAÇÃO DE DADOS

ORGANIZAÇÃO ALVO

Uma empresa de consultoria de 10 pessoas enviou uma pequena equipa para a Hungria para concluir um projeto de cliente. Durante a sua estadia, o consultor sénior deixou o seu portátil de trabalho, que tinha acesso a informações sensíveis do cliente e detalhes bancários da empresa, num carro trancado enquanto geria um emprego. O carro foi assaltado e o portátil foi roubado. Infelizmente, os dados no pc não foram encriptados porque o colaborador não aplicou a política da empresa para encriptar todos os dados sensíveis no seu computador. A empresa tinha agora medo de um ciberataque aos seus sistemas, contas bancárias e fugas de dados dos clientes.

Tipo de ataque: Roubo físico de um pc não encriptado. A encriptação é o processo de baralhar texto legível para que só possa ser lido pela pessoa que tem a chave de desencriptação. Cria uma camada adicional de segurança para informações sensíveis.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

As informações necessárias para descrever o incidente foram recolhidas através de uma entrevista com o consultor sénior da empresa e o técnico de TI da empresa de TIC que apoia a empresa de consultoria. A interação foi realizada com a condição de manter informação sensível anonimamente. Mesmo que o entrevistado estivesse disposto a descrever o incidente, algumas informações de encriptação não podiam ser obtidas e esta é a razão pela qual foi solicitado à empresa de TIC de apoio para esclarecer o caso..

PREVENIR

Embora o incidente não seja um claro incidente de ciberataque, é um incidente sério e muito comum que causa uma série de ataques cibernéticos significativos.

No caso da empresa analisada, na perspetiva da cibersegurança, operavam políticas e mecanismos específicos, mas estas não foram implementadas por alguns colaboradores devido à sua baixa experiência no domínio da informação e dos riscos de cibersegurança.

IDENTIFICAR

O funcionário reportou imediatamente o roubo à polícia e à sua empresa. O banco foi ainda informado para monitorizar as transações de conta. A empresa informou, em conformidade, a empresa de apoio às TIC para desativar o acesso remoto do portátil e começou a monitorizar a atividade. O portátil estava equipado com ferramentas de segurança e proteção de senhas. Os dados armazenados no disco rígido não foram encriptados – isto incluía dados sensíveis, dados dos clientes e dados bancários da empresa.

Para uma identificação com base no comportamento deste ataque, podem ser utilizadas as seguintes técnicas MITRE ATT&CK:

- ☑ T1027 - Obfuscated Files or Information
- ☑ T1036 – Masquerading
- ☑ T1586.002 – Compromise Accounts: Email Accounts

RESPONDER

Resposta: A empresa deve seguir as leis estatais no que diz respeito a uma violação de dados. As leis estatais e os regulamentos da UE em matéria de GPDR são muito rigorosos com multas de alto custo.

- ☑ **QUEM:** O agressor não pôde ser identificado. Só o local do incidente era conhecido..
- ☑ **A QUEM:** alvo não especificado
- ☑ **PORQUÊ:** Recolha de dados sensíveis e obtenção de dinheiro com a venda do equipamento roubado
- ☑ **O QUÊ:** Dados sensíveis dos clientes e dados bancários da empresa
- ☑ **COMO:** perda de equipamentos, fugas de dados sensíveis e ataque de conta bancária
- ☑ **ESTRATÉGIA:** A ameaça começou num computador sem antivírus e espalhou-se lateralmente. Um processo de limpeza foi realizado por uma empresa especializada em TI&C.

RECUPERAR

IMPACTO: A empresa de consultoria gastou mais de 20.000 euros na implementação, monitorização e melhorias operacionais. Uma violação de dados tem impacto negativo numa marca e a confiança tem de ser reconstruída.

As principais consequências do ataque foram as seguintes:

- ☑ Perda de dados
- ☑ Perda de PC
- ☑ Compromisso do sistema
- ☑ Custos financeiros

RECUPERAR: A estratégia de recuperação centrou-se em minimizar a reputação da marca e monitorizar e controlar os sistemas internos e contas bancárias da empresa. Preventivamente, todas as credenciais de conta bancária mudaram, e os privilégios dos sistemas dos funcionários foram suspensos e alterados.

ESTRATÉGIA: A empresa deve implementar várias ações para prevenir tais incidentes. A sua estratégia deve concentrar-se em

- ☑ Programas de fromação para a consciencialização dos colaboradores
- ☑ Realizar verificações e auditorias regulares
- ☑ Prevenção da Execução e implementação de um sistema de gestão de riscos

LIÇÕES APRENDIDAS

- ☑ As empresas devem criar e formar trabalhadores sobre o manuseamento seguro de dispositivos de trabalho.
- ☑ Os dispositivos devem ser armazenados com segurança quando não estiverem presentes na presença imediata do trabalhador.
- ☑ As empresas devem tomar medidas para encriptar os dados onde quer que seja armazenado ou transmitido.
- ☑ Os colaboradores devem ter uma compreensão clara da importância da encriptação e como usá-la.
- ☑ As empresas devem compreender e conhecer as suas responsabilidades ao abrigo das leis de notificação de violação de dados do país em que operam.
- ☑ Uma revisão regular das práticas de segurança da empresa é imperativa nas organizações modernas para prevenir incidentes, descobrir vulnerabilidades e reduzir o impacto dos incidentes.

"Houve um aumento de 57% nas variantes de botnets mirai identificadas em 2019. As variantes de Mirai são normalmente usadas para ataques de força bruta em dispositivos IoT. Estes ataques aumentaram 51%, enquanto as explorações web aumentaram 87% em 2019." (MCCART, 2022).

ESTUDO DE CASO 18: ATAQUE DO DDOS TRAVA SERVIÇOS IMPORTANTES

ORGANIZAÇÃO ALVO

A organização visada era uma empresa de acolhimento. Os agressores empataram um ataque de negação de serviço distribuído contra um site específico em meados de dezembro de 2021, superando uma largura de banda de 1,5 gigabits por segundo e quase 100 milhões de pacotes por segundo, o maior ataque enfrentado por uma empresa host.

A empresa acredita que o atacante se focou nos sites com jogos de casino online, e o fornecedor de hospedagem não era o alvo real. Ataque do DDOS provoca o fim da disponibilidade dos serviços do cliente por mais de 12 horas.

Um ataque de negação de serviço distribuído (DDoS) é uma tentativa maliciosa de perturbar o tráfego normal de um servidor, serviço ou rede direcionado, esmagando o alvo ou a sua infraestrutura circundante com uma inundação de tráfego de Internet. Os ataques DDoS alcançam a eficácia utilizando vários sistemas

informáticos comprometidos como fontes de tráfego de ataque. As máquinas exploradas podem incluir computadores e outros recursos em rede, tais como dispositivos IoT.

COMO FOI ADQUIRIDA A INFORMAÇÃO?

A informação necessária para descrever este ciberataque foi recolhida através de duas entrevistas (reuniões presenciais), uma com o CEO da empresa e outra com um engenheiro de TI da empresa. Ambos estavam dispostos a descrever e dar detalhes do incidente, mas pediram para manter anónimos tanto as empresas como os seus nomes porque a informação era demasiado sensível para eles.

PREVENIR

Embora o fornecedor de hospedagem tenha vários procedimentos e mecanismos de segurança cibernética, parece que os atacantes encontraram um ponto vulnerável para explorar.

O técnico da empresa notou que o site subitamente se tornou lento, mas assumem que se acabou por ser um pico legítimo no tráfego devido à época de férias. O ataque foi identificado logo após o site ficar indisponível e o cliente queixou-se.

IDENTIFICAR

Os agressores usaram o tráfego de fontes em todo o mundo. Parece que o ataque de negação de serviço foi criado por um botnet Mirai. E como o botnet Mirai tem a capacidade de enviar cerca de 600 megabits por segundo, eles usaram um ataque de segundo nível com um botnet Mirai diferente.

Mirai é um malware que infeta dispositivos inteligentes que funcionam em processadores ARC, transformando-os numa rede de bots ou "zombies" controlados remotamente. Esta rede de bots, chamada botnet, é frequentemente usada para lançar ataques DDoS.

O fornecedor de alojamento usou ferramentas de análise de tráfego para identificar o ataque. A característica básica do ataque é o elevado volume proveniente da mesma série de endereços IP. Os engenheiros conseguem isolar os IPs e o site voltou.
Depois disso, tentam identificar porque é que a ferramenta de análise de tráfego não detetou o ataque desde as primeiras fases..

De acordo com o quadro MITRE ATT&CK, esta incidência pode ser descrita da seguinte forma:

- ☑ T1499 - Negação de Serviço endpoint
- ☑ T1498 - Negação de Serviço de Rede

RESPONDER

- ☑ **QUEM:** O atacante não foi identificado. O ataque veio de todo o mundo.
- ☑ **A QUEM:** O alvo era um site específico que hospedava jogos de casino online.
- ☑ **PORQUÊ:** Para interromper a sua operação.
- ☑ **O QUÊ:** Site da empresa.
- ☑ **COMO:** Ataque de DDOS com botnets de Mirai.

☑ **ESTRATÉGIA:** O ataque começou com um fornecedor de hospedagem para interromper a operação de um site específico. A ferramenta analítica de tráfego não alertou para a possibilidade de um ciberataque. A empresa aumentou a sensibilidade dos alarmes na ferramenta de análise de tráfego para evitar incidentes semelhantes no futuro.

RECUPERAR

IMPACTO: O fornecedor de alojamento teve custos extra significativos para cobrir o ataque e também, eles tinham graves danos de reputação. Tinham o custo extra da mão-de-obra para recuperar o website e as sanções sobre o acordo SLA com o cliente. O custo total foi estimado em aproximadamente 40.000 euros.

RECUPERAÇÃO: A estratégia de recuperação centrou-se em isolar os IPs de ataque para parar o ataque e recuperar o funcionamento do site. Outras ações foram, para aumentar a sensibilidade dos alarmes da ferramenta analítica de tráfego. Verifique todos os servidores e serviços de hospedagem para quaisquer outros ataques ou atividades suspeitas.

ESTRATÉGIA: A empresa deve implementar várias ações para prevenir tais incidentes. A sua estratégia deve concentrar-se em

☑ Aumentar a sensibilidade da ferramenta analítica de tráfego
☑ Instale uma segunda ferramenta para segurança extra
☑ Realizar programas de formação para assegurar a consciencialização dos colaboradores
☑ Restringir algumas gamas de IP
☑ Realizar verificações e auditorias regulares
☑ Prevenção da Execução e implementação de um sistema de gestão de riscos
☑ Certificar as suas infraestruturas e serviços nas ISO27001 e ISO22301.

LIÇÕES APRENDIDAS

☑ A perturbação vem de várias formas. Perturbações ou atrasos podem surgir de várias formas, especialmente para os fornecedores de hospedagem. Quando um ataque é identificado, as equipas de resposta apropriadas devem dedicar recursos para lidar com ele.
☑ Muitos ciberataques são facilmente evitáveis. Ciberataques sofisticados podem causar muitos danos, mas muitos deles podem ser facilmente evitados com a segurança certa no lugar. É importante fazer um sistema de gestão de segurança forte e proactivo para parar os ataques. Este sistema de gestão requer manutenção contínua, monitorização de todos os sistemas e dispositivos da rede, incluindo a atualização da tecnologia e a aplicação de patches de segurança para explorações conhecidas.
☑ Os ataques do DDoS devem ser levados a sério. Os ataques do DoS e DDoS de hoje são diferentes, visto que são mais viciosos, pontiagudos e capazes.
☑ Sem limite de tempo. Os ataques em camadas de rede podem durar mais de 48 horas, enquanto os ataques da camada de aplicação podem durar dias. Infiltração de sistemas e redes para espionagem — semanas e meses.

☑ A cibersegurança deve ser uma prioridade. A cibersegurança deve ser uma das maiores prioridades para todas as entidades que operam no panorama atual. Estes ataques tornaram-se sofisticados, direcionados, capazes e não regulamentados. Umaameaça de ll deve ser levada a sério, incluindo os ataques DDoS, que estão a tornar-se cada vez mais comuns.

CONCLUSÃO

Com base no portfólio diversificado que é apresentado dentro da bateria documental ENCRYPT 4.0 em ciberataques, as seguintes conclusões poderiam ser retiradas:

- ☑ Com o desenvolvimento das TIC e no contexto da Indústria 4.0, a cibersegurança tem uma importância crescente e **as empresas que carecem de uma defesa cibernética adequada estão a colocar as suas operações em sério risco.**
- ☑ **Os colaboradores desempenham um papel fundamental na ciberdefesa**, pelo que os colaboradores, tanto no seio das PME como das grandes empresas, devem receber pelo menos formação básica sobre como proteger os dados das empresas e trabalhar com informação sensível, uma vez que mais do que muitos ciberataques acontecem devido à falta de conhecimento sobre estes aspetos, especialmente no contexto do trabalho remoto durante a pandemia COVID-19.
- ☑ **As PME que desconsideram o sector em que operam estão** a **tornar-se alvos primários para os hackers e cibercriminosos organizados**, mas, ao mesmo tempo, apenas 1/3 das PME têm um plano para conter um potencial ciberataque, pelo que as PME precisam de prever a cibersegurança como prioridade máxima para garantir a sua competitividade a longo prazo.

REFERÊNCIAS

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

2. Barber, B., 2016. William Hill apologise after website attack. [Online] Racing Post. Disponível em: https://www.racingpost.com/news/william-hill-apologise-after-website-attack/266196 (ESTUDO DE CASO 6)

3. Blue goose, n.d. Information Security at William Hill. [Online] blue goose. Disponível em: https://bluegooseis.co.uk/work/william-hill (ESTUDO DE CASO 6)

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

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

7. Cyber Startup Observatory. Disponível em: https://cyberstartupobservatory.com/ (ESTUDO DE CASO 4)

8. CyberNews, 2021. Thousands of Humana customers have their medical data leaked online by threat actors. [Online] 2022 Cybernews. Disponível em: https://cybernews.com/news/humana-insurance-customers-medical-data-leaked/ (ESTUDO DE CASO 5)

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

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

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

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

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

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

20. VentureBeat, 2022. Report: Average time to detect and contain a breach is 287 days. [Online] VentureBeat. Disponível em: 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. Disponível em: 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. Disponível em: https://lab.wallarm.com/the-biggest-hacker-attacks-on-gambling/ (ESTUDO DE CASO 6)

ENCRYPT 4.0

Cofinanciado pelo Programa Erasmus+ da União Europeia

PARCEIROS DO PROJETO

ENCRYPT 4.0

Apoiar a Indústria Europeia Através da Capacitação de Profissionais de Cibersegurança

O Projeto ENCRYPT4.0 (2020-1-RO01-KA202-079983) tem como objetivo e fabricar a gestão das PME para adotar uma abordagem proativa em relação à cibersegurança, apoiando-as no processo de análise, identificação e combate aos riscos e ameaças cibernéticas aplicáveis à sua organização. Através da elaboraçãode uma aprendizagem interativa baseada em projetos no que diz respeito ao reforço das competências e competências de cibersegurança dos colaboradores das PME ou/e profissionais de cibersegurança.

"George Emil Palade" Universidade de Medicina, Farmácia, Ciências e Tecnologia de Târgu Mureş - Roménia

Coordenador do projeto

European Center for Quality Ltd., Empresa de consultoria - Bulgária

Instituto de Soldadura e Qualidade, Instituição tecnológica - Portugal

Avantalia, PME tecnologica - Espanha

FH Joanneum, Universidade de Ciências Aplicadas - Áustria

PCX Management, Computadores & Sistemas de Informação Ltd. - Chipre