Cofinanciado pela
União Europeia

EYESonCS

EyesOnCS
Compêndio de Riscos de Cibersegurança

Português
Outubro 2023

Projeto
Acrónimo: EyesOnCS
Título: Enhancing Cyber Security – Development of trainings using "Escape Room" Model
Project nº: 2021-1-DE02-KA220-VET-000033003
Duração: 01. Gennaio 2022 - 31. Dicembre 2023 (24 mesi)
Programa: Ação-Chave 2: Parcerias de cooperação no domínio do ensino e da formação profissionais

Coordenador do projeto: Fachhochschule des Mittelstands (FHM)

Edição: Outubro 2023

Parceiros do projeto

Staatlich anerkannte, private Fachhochschule des Mittelstands (FHM)

virtualcampus

AKADEMIE ASW

fb finance & banking Associazione per lo sviluppo organizzativo e delle risorse umane

Fique atento!

Siga-nos
Saiba mais sobre o projeto em:

www.eyesoncs.eu

Cofinanciado pela União Europeia

Financiado pela União Europeia. Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidos como responsáveis por essas opiniões.

Tabela de Conteúdos

Figuras

1. Introdução

Não há um dia em que não exista cibercrime. A situação da cibercriminalidade em todo o mundo aumentou significativamente nos últimos anos. Uma das razões é a digitalização em curso em quase todas as esferas do trabalho e da vida. Enquanto no passado os crimes e ataques se caracterizavam por um assalto a um banco ou outro ataque físico, atualmente caracterizam-se por um atacante sentado numa praia com um computador portátil e que obtém acesso ilegal ao sistema de distribuição de um banco para extorquir um resgate. A associação do sector Bitcom contabiliza mais de 220 mil milhões de euros de prejuízos por ano. Para as pequenas e médias empresas, um ataque e a obtenção de segredos comerciais podem significar a ruína económica (Streim, A., Mann, S. (2021)). A pandemia do coronavírus também permitiu novos formatos de trabalho num curto espaço de tempo. As medidas de proteção correspondentes não foram estabelecidas ou adaptadas em paralelo. Isto abre caminhos para ataques à segurança e vulnerabilidades para invasores e infractores. Por este motivo, é extremamente importante informar os trabalhadores sobre os efeitos e as consequências de um ciberataque e sensibilizá-los em conformidade.

Este compêndio foi desenvolvido no contexto do projeto Erasmus+ "EyesOnCS". A equipa do projeto tem vários objetivos com o desenvolvimento desta publicação: Primeiro, uma visão geral é introduzir estratégias para a aplicação da cibersegurança (CS), especialmente nas PME. Em seguida, discute os desafios específicos enfrentados pelas PME na implementação da cibersegurança. Posteriormente, o compêndio centra-se brevemente na importância da educação e da formação para evitar ataques de cibersegurança. Segue-se uma recolha exaustiva de casos de cibersegurança ocorridos na prática. Estes casos foram recolhidos pela equipa internacional do projeto junto de empresas e outras instituições e estão documentados em pormenor para efeitos do presente compêndio.

Após uma introdução ao tema da segurança em geral, o segundo capítulo trata de importantes estratégias nacionais e europeias de SC. Neste contexto, é explicado e destacado o papel da ENISA (Agência da União Europeia para a Cibersegurança). A este respeito, o Relatório Anual de Actividades Consolidado da ENISA refere: "Em 2021, a ENISA foi confrontada com os desafios trazidos pela pandemia, que afectou as actividades de reforço de capacidades a vários níveis. Por um lado, vários cursos e exercícios tiveram de ser convertidos para serem ministrados em linha, por razões óbvias. Esta mudança colocou alguns desafios desde a conversão".[1]

1 ENISA: Consolidated Annual Activity Report 2021, Attiki, 2022

Além disso, o compêndio centra-se, neste capítulo, na Lei da Cibersegurança da UE, que introduz um quadro de certificação da cibersegurança a nível da UE para produtos, serviços e processos das tecnologias da informação e da comunicação (TIC). As empresas com atividade na UE beneficiarão do facto de terem de certificar os seus produtos, processos e serviços de TIC apenas uma vez e de verem os seus certificados reconhecidos em toda a União Europeia.[2] Além disso, neste segundo capítulo, o compêndio tenta registar e apresentar várias estratégias de segurança nacionais. Por razões práticas, a lista não é exaustiva. São explicadas, entre outras, as seguintes:

- a associação alemã "Deutschland sicher im Netz e.V. (DsiN)"[3]
- o CERT-Bund[4], uma equipa de resposta a emergências informáticas para as autoridades federais
- a Estratégia Nacional de Cibersegurança italiana para 2022/26
- o Centro Nacional de Cibersegurança (CNCS) português.

O terceiro capítulo resume os desafios para as PME no que respeita à cibersegurança. Para o efeito, os autores utilizam a abordagem tripla da ENISA, incluindo recomendações para as PME[5]:

- Área Pessoas
- Área de processos
- Área técnica.

Este projeto visa implementar recomendações específicas para as PME a nível educativo. As recomendações da ENISA para as PME6 centram-se em três domínios diferentes. Este compêndio enumera um conjunto de questões orientadoras para os controlos de segurança e também para a avaliação dos casos práticos de segurança recolhidos (ver capítulo 5).

Além disso, o projeto visa o desenvolvimento de métodos especiais de formação virtual em segurança social e a sua implementação com base nos chamados cenários. Assim, no capítulo 4 do compêndio, descrevem-se e avaliam-se conceitos relevantes para a formação em segurança social. Estes incluem a aprendizagem baseada em jogos e as salas de fuga educativas (EER).

Uma parte particularmente importante e extensa do compêndio consiste na descrição sumária e na avaliação de casos práticos de SC que os parceiros do projeto pesquisaram, compilaram e avaliaram nos seus respectivos países de origem, Itália, Alemanha e Portugal. O Capítulo 5 descreve 26 desses casos práticos numa forma uniformemente estruturada e comparativa.

---

2 UR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 32019R0881 - EN - EUR-Lex.
3 Deutschland sicher im Netz, https://www.sicher-im-netz.de.
4 Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html.
5 ibid.

2. Estratégias Nacionais e Europeias

A nível europeu, as estratégias de prevenção do cibercrime e de segurança cibernética estão ainda em desenvolvimento. Já existem algumas boas abordagens, contudo existem ainda muitas tarefas desafiantes. Atualmente, existem apenas algumas agências governamentais que abordam esta questão, o que é particularmente importante para as PMEs.

Uma destas agências é a AESC (Agência Europeia para a Segurança Cibernética)[6] que tem a tarefa de contribuir para um elevado nível comum de cibersegurança em toda a Europa. A AESC apoia activamente a política da União Europeia para aumentar a cibersegurança e a fiabilidade dos produtos e serviços das tecnologias de informação e comunicação através da certificação de cibersegurança. Além disso, a Agência contribui para tornar a infra-estrutura da União mais defensável e, em última análise, para garantir um ambiente digital seguro para a sociedade europeia e os cidadãos.

A anterior pandemia do Covid-19 aumentou ainda mais a atividade dos cidadãos europeus em várias redes, tais como a Internet, tanto em ambientes profissionais como privados. Infelizmente, a pandemia abriu mais portas de entrada para métodos de ataque coordenados e adaptados. Para os atacantes ciber-criminosos, isto tem sido cada vez mais fácil devido à falta de estruturas de defesa, know-how e mecanismos de defesa distintos. A AESC aprendeu com isto e, por conseguinte, intensificou significativamente mais uma vez as suas atividades de combate ao crime. A este respeito, o Relatório Anual Consolidado de Actividades da AESC diz: "Em 2021, a AESC foi confrontada com os desafios trazidos pela pandemia, que afectou as actividades de construção de capacidades a múltiplos níveis. Por um lado, vários cursos e exercícios tiveram de ser convertidos para entrega em linha, por razões óbvias. Esta mudança colocou alguns desafios desde a conversão".[7]

Em 2019, a Agência da UE para a Segurança Cibernética tornou-se mais forte através da Lei de Segurança Cibernética da UE.[8] Esta concede um mandato permanente à agência e confere-lhe mais recursos e novas tarefas. Agora, a AESC terá um papel fundamental na criação e manutenção do quadro europeu de certificação de cibersegurança, preparando o terreno técnico para esquemas de certificação específicos. Supervisiona a informação do público sobre os esquemas de certificação e os certificados emitidos através de um website dedicado. Além disso, a AESC está mandatada para aumentar a cooperação operacional a nível da UE, ajudando os Estados-Membros da UE que desejem solicitá-la a lidar com os seus incidentes de cibersegurança, e apoiando a coordenação da UE em caso de ciberataques e crises transfronteiriças em grande escala.

6 https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity
7 ENISA: Consolidated Annual Activity Report 2021, Attiki, 2022
8 EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 320 19R0881 - EN - EUR-Lex.

Além disso, a Lei de Segurança Cibernética da UE introduz um quadro de certificação de segurança cibernética a nível da UE para produtos, serviços e processos das tecnologias da informação e da comunicação (TIC). As empresas que fazem negócios na UE beneficiarão de ter de certificar os seus produtos, processos e serviços de TIC apenas uma vez e ver os seus certificados reconhecidos em toda a União Europeia. O quadro de certificação de cibersegurança da UE para produtos TIC permite a criação de esquemas de certificação da UE adaptados e baseados no risco. Fornece esquemas de certificação à escala da UE como um conjunto abrangente de regras, requisitos técnicos, normas, e procedimentos. O quadro será baseado no acordo a nível da UE sobre a avaliação das propriedades de segurança de um produto ou serviço específico baseado em TIC. Atestam que os produtos e serviços TIC que foram certificados em conformidade com tal esquema cumprem os requisitos especificados.[9]

A nível nacional na **Alemanha**, a associação Deutschland sicher im Netz e.V. (DsiN)"[10]apoia os consumidores e as pequenas empresas a lidar de forma segura e confiante com o mundo digital, bem como a oferecer oportunidades de aprendizagem para pessoas em ambientes privados e profissionais.
Outro apoio muito útil para as PMEs é o CERT-Bund[11], a Equipa de Resposta a Emergências Informáticas das autoridades federais, que é o ponto central de contacto para medidas preventivas e reativas em caso de incidentes relacionados com a segurança nos sistemas informáticos. Para além do apoio às autoridades federais, o cidadão CERT fornece informação gratuita e neutra sobre ataques atuais por malware, bem como sobre vulnerabilidades de segurança em aplicações informáticas.

Em Maio de 2022, **Itália** anunciou a sua Estratégia Nacional de Segurança Cibernética para 2022/26, um documento crucial para enfrentar as ameaças cibernéticas e aumentar a resiliência do país. A estratégia, desenvolvida pela Agência Nacional Italiana de Segurança Cibernética, inclui 82 objectivos, e visa enfrentar os seguintes desafios:

- Assegurar uma transição digital cyber-resiliente da Administração Pública (AP) e do sistema produtivo.
- Prever a evolução das ameaças cibernéticas para reduzir o seu impacto nas infra-estruturas e organizações nacionais.
- Prevenir a desinformação em linha num contexto mais amplo da ameaça híbrida.
- Gerir as crises cibernéticas.
- Reforçar a autonomia do sector digital estratégico nacional e europeu.

A estratégia italiana de cibersegurança combina segurança e desenvolvimento, em conformidade com os valores da nossa Carta Constitucional, tem em consideração as disposições da estratégia de cibersegurança da União Europeia de Dezembro de 2020, a bússola estratégica da UE para a segurança e defesa de Março de 2022 e as recentes

9 European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

10 Deutschland sicher im Netz, https://www.sicher-im-netz.de.

11 Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

orientações estratégicas da NATO. Para alcançar esta nova visão, a Itália concebeu um ecossistema de cibersegurança baseado na colaboração entre os sectores público e privado. Num tal sistema, a contribuição activa das Instituições é complementada pela dos operadores económicos - principalmente os encarregados da gestão de infra-estruturas das quais depende a prestação de serviços essenciais pelo Estado - o mundo das universidades e da investigação, e também a sociedade civil.[12]

Em **Portugal**, o Centro Nacional de Cibersegurança (CNCS) é o coordenador operacional e autoridade nacional portuguesa especializada em cibersegurança, trabalhando com entidades estatais, operadores de serviços essenciais e fornecedores de serviços digitais, assegurando que o ciberespaço é utilizado como um espaço de liberdade, segurança e justiça, para a protecção de todos os sectores da sociedade.[13] A missão do CNCS é contribuir para a utilização livre, fiável e segura do ciberespaço em Portugal, através da melhoria contínua da cibersegurança nacional e da cooperação internacional, em coordenação com todas as autoridades competentes, e da implementação de medidas e instrumentos necessários para a antecipação, detecção, reação e recuperação de situações que possam comprometer o funcionamento de infra-estruturas críticas e interesses nacionais. O CERT.PT coordena a resposta a incidentes envolvendo entidades estatais, operadores de infra-estruturas críticas, operadores de serviços essenciais, fornecedores de serviços digitais, e, em geral, o ciberespaço nacional em Portugal.

3. Desafios das PMEs

Os ciberataques podem colocar os negócios das pequenas e médias empresas em risco de extinção/término. As PME são frequentemente empresas familiares, cujos segredos de produção e comerciais se baseiam numa longa tradição. Na prática, isto está frequentemente em contraste considerável com as medidas de protecção prevalecentes, que estão normalmente associadas a custos consideráveis para as PMEs e/ou carecem do know-how correspondente. O número de ciberataques às PMEs têm aumentado exponencialmente nos últimos três anos. Estão também a tornar-se cada vez mais objecto de espionagem económica e industrial orientada. O conhecimento temático básico é familiar aos funcionários de grupos empresariais com os seus próprios departamentos de segurança empresarial. Têm um certo nível de conhecimento e recebem formação interna a intervalos regulares. No caso de um ataque, as responsabilidades e os procedimentos são nomeados e ensaiados. Todas estas estruturas não estão geralmente implementadas nas PMEs. A maioria dos funcionários geralmente não sabe como lidar com dados sensíveis. Isto não só compromete a capacidade de uma empresa de fazer negócios, mas

12 ACN Italy: National Cybersecurity Strategy 2022 – 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, seen 29.7.22
13 Cyber security intelligence: National Cyber Security Centre Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html.

também, na pior das hipóteses, muitos postos de trabalho. Afinal de contas, as PMEs também fazem parte da cadeia de fornecimento. Um ataque cibernético bem sucedido a uma PME pode, portanto, ter também um grande impacto na cadeia de abastecimento, assim como numa agência governamental ou noutras empresas de maior dimensão.

De acordo com um inquérito[14] recente, mais de 80% das PME europeias declararam que as questões de cibersegurança teriam um sério impacto negativo nos seus negócios no prazo de uma semana após a ocorrência dos problemas, dos 57% que afirmaram que muito provavelmente entrariam em falência ou cessariam a sua actividade. Apesar disso, as PMEs não parecem compreender que a cibersegurança não é algo que tenha impacto apenas nas organizações de maior dimensão. Por conseguinte, as PMEs precisam de estar conscientes do impacto que as questões de cibersegurança podem ter nos seus negócios. Muitas PMEs acreditam que os controlos de segurança incluídos nos produtos informáticos que adquirem são suficientes e que não são necessários controlos de segurança adicionais, a menos que sejam exigidos por regulamento ou lei. Este compêndio destina-se a ajudar a proporcionar maior clareza a este respeito. Por conseguinte, a ENISA propõe uma abordagem tripla que inclui recomendações para as PME[15]:

- Área Pessoas
- Processos de Área
- Área Técnica.

Este projecto visa implementar as seguintes recomendações de PMEs a nível educacional. Estas incluem manter o software atualizado, aplicar regras rigorosas de controlo de acesso, fazer uso de serviços de nuvem e muito mais.

As recomendações[16] da ENISA às PMEs centram-se em quatro áreas diferentes. Dentro das áreas estão listados os principais pontos de controlo, incluindo as principais questões. Esta lista pode também ser utilizada como um questionário para um auto-teste.

14 ENISA: Cybersecurity for SMES- Challenges and Recommendations, European Union Agency for Cybersecurity (ENISA), Attiki, 2021
15 ibid.
16 ibid.

Questões Orientadoras para a Área PESSOAS

Responsabilidade	Um diretor, ou equivalente, tem responsabilidade pela cibersegurança?
Adesão do Funcionário	Será que todos os funcionários reconheceram por escrito que leram, compreenderam e aceitaram a política de segurança da informação?
Consciencialização do Funcionário	Todos os utilizadores dos sistemas informáticos recebem formação regular sobre as suas responsabilidades de segurança sobre como identificar e lidar com várias ameaças à segurança? Assegure-se de que os funcionários estão cientes e podem verificar todos os pontos de contacto e canais de comunicação.
Formação de Cibersegurança	Os funcionários com responsabilidades específicas de segurança recebem formação adequada e regular para apoiar o seu papel?
Políticas de Cibersegurança	Tem uma política de segurança documentada, com procedimentos operacionais associados, assinada e totalmente apoiada pela gestão de topo?
Gestão de Terceiros	A direcção autoriza o acesso de terceiros a informações confidenciais e/ou comercialmente sensíveis enquanto se aguarda o preenchimento de formulários de confidencialidade adequados?

Pergunta orientadora para Área PROCESSO

Auditorias	Os sistemas críticos, tais como firewalls e routers, são regularmente testados quanto à sua vulnerabilidades? Os computadores são verificados para garantir que não existem cópias de software ilegal?
Planeamento e resposta a incidentes	Existe um plano para lidar com incidentes de segurança?
Palavras-passe	Todas as palavras-passe padrão em todos os sistemas são reiniciadas a partir das palavras-passe padrão do fornecedor instalado? Os utilizadores são forçados a utilizar palavras-passe complexas e difíceis de adivinhar?

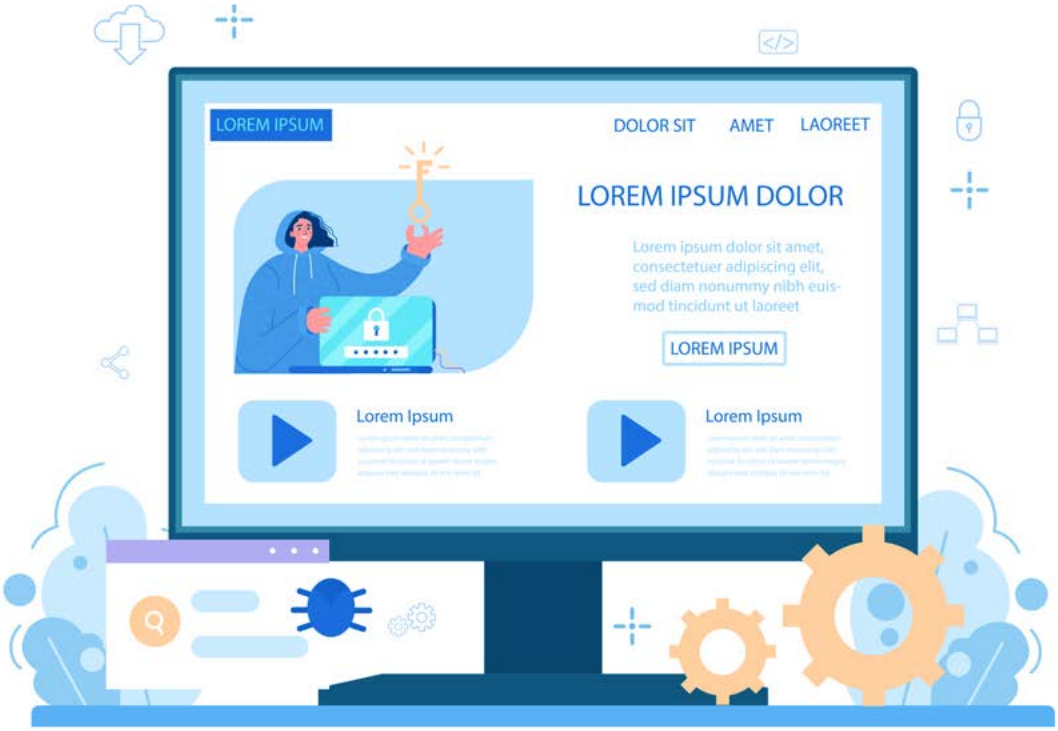
Correcções de software	Existe um mecanismo para assegurar que os patches de segurança críticos sejam colocados nos sistemas de forma atempada e auditada?
Proteção de dados	Os sistemas e bases de dados que armazenam dados pessoais estão devidamente protegidos para garantir o cumprimento dos requisitos regulamentares e legais, tais como o Regulamento Geral de Protecção de Dados da UE, a Lei de Cibersegurança[17] e a Lei de Protecção de Dados?

Pergunta Orientadora para a ÁREA TÉCNICA

Rede de segurança	As ligações externas, tais como à Internet, são autorizadas pela direcção, devidamente documentadas e asseguradas através de Firewalls?
Anti-Vírus	Todos os sistemas informáticos estão protegidos com o software antivírus mais atualizado? Os utilizadores são instruídos sobre como identificar e lidar com e-mails ou ficheiros suspeitos que possam conter vírus informáticos?
Criptografia	Todos os dispositivos que armazenam dados têm encriptação de disco completa aplicada? Utiliza Redes Privadas Virtuais (VPNS) quando comunica através da Internet em redes públicas?
Monitorização da segurança	Os ficheiros de registo de dispositivos de segurança importantes são activamente monitorizados para detectar potenciais falhas de segurança?
Segurança física	• Os recursos informáticos críticos, tais como servidores de ficheiros, estão protegidos numa área segura contra o acesso não autorizado? • Estão em vigor medidas de escritório em casa que garantem áreas seguras comparáveis às do escritório (portas fechadas ao sair do local de trabalho, sem acesso de terceiros à informação através de janelas ou de outra forma)?
Cópias de segurança seguras	Uma boa cópia de segurança pode salvar o seu negócio de um ataque de resgate. Faz regularmente cópias de segurança de dados e sistemas críticos para proteger o armazenamento offline? Testa regularmente a restauração a partir das suas cópias de segurança para verificar se consegue recuperar totalmente os seus dados e sistemas?

17 European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

4. Papel da educação e da formação - Conceitos relevantes para a Formação em Cibersegurança



O facto de a cibersegurança bem sucedida depender não só da protecção técnica, mas também, em grande medida, da sensibilização e confiança dos funcionários em agir nem sempre é reconhecida pelas empresas. Embora uma em cada quatro empresas identifique continuamente a necessidade de ação em matéria de segurança empresarial e disponibilize mais recursos, o foco está claramente na protecção técnica. Nas PMEs, a formação e sensibilização dos funcionários realiza-se frequentemente apenas de forma limitada. Isto significa que é dada muito pouca atenção ao factor de protecção humana, que se torna ainda mais importante com o teletrabalho. A sensibilização para os riscos de segurança associados aos locais de trabalho flexíveis está a ganhar importância. Obviamente, é importante sensibilizar as empresas para as novas oportunidades de ataques que podem surgir com o teletrabalho.
Por conseguinte, é aconselhável oferecer cursos de formação que incidam sobre este tema. Além disso, é valioso sensibilizar as empresas com informações escritas ou palestras de instituições.

4.1 Aprendizagem baseada em jogos

Os video-jogos apareceram no mercado de consumo há cerca de 50 anos e o seu impacto na sociedade cresceu constantemente até se tornar um elemento social e cultural fundamental (Oblinger 2006). Os jogos são sistemas endógenos, com atividades de resolução de problemas estruturadas pela mecânica dos jogos e regras do jogo. O envolvimento em jogos e brincadeiras é motivado internamente, no sentido em que os indivíduos participam neles voluntariamente. Os jogos descrevem a interação entre o jogador e os elementos do jogo que conduzem a comportamentos diferentes e produzem resultados diferentes. Em grande medida, os jogos envolvem a avaliação das escolhas do jogador que promove a sua imersão, um fenómeno vivido por um indivíduo quando este se encontra num estado de profundo envolvimento mental (Agrawal et al, 2020). Mas os jogos também contribuem para a socialização e para ajudar os jogadores a estabelecer ligações entre a causa e o efeito das suas decisões, o que pode contribuir para o pensamento crítico e lógico. Também melhoram várias competências cognitivas, intrapessoais e interpessoais como a perceptividade, atenção, memória, análise e síntese visual e auditiva, comparação, classificação, e generalização.

Embora inicialmente pensado como simples objectos de entretenimento, a concepção e/ou utilização de videojogos para outros fins foi visto como um passo lógico para tirar partido da motivação e envolvimento que os utilizadores experimentam enquanto jogam. Como tal, os videojogos são agora utilizados para educação e formação, sensibilização, publicidade, estudos de investigação, campanhas de saúde pública, etc. Estes jogos, chamados Jogos Sérios, são genericamente definidos como "[jogos] que não têm entretenimento, divertimento ou diversão como objectivo principal" (Michael e Chen 2006, p. 21) ou como "... um concurso mental, jogado com um computador de acordo com regras específicas, que utiliza entretenimento para promover a formação governamental ou empresarial, educação, cuidados de saúde, consciência social, políticas públicas, gestão de crises e objectivos estratégicos de comunicação" (Zyda 2005, p. 26). Os jogos sérios exploram a motivação inerente e a imersão dos jogadores através da utilização de mecânica e dinâmica de jogo adequada para desenvolver aptidões e competências específicas, para transmitir uma informação (ou mensagem) desejada ao utilizador ou para reforçar o conhecimento ou a consciência adquirida enquanto o utilizador está imerso num ambiente divertido.

A educação é a área com mais exemplos (bem sucedidos) da utilização de jogos sérios, gerando assim o termo "aprendizagem baseada em jogos", que se centra no desenvolvimento de jogos concebidos tendo em mente objectivos de aprendizagem específicos. Os utilizadores podem "aprender fazendo" e "aprender por erro" num ambiente controlado que apoia o desenvolvimento de conhecimentos, aptidões e competências e pode mesmo melhorar o trabalho de equipa, as capacidades sociais, a liderança e a colaboração (Juzeleniene et al. 2014).

A Aprendizagem Baseada em Jogos visa extrair componentes que tornam os jogos apelativos e combiná-los com a informação e conhecimentos desejados a serem transmitidos ao utilizador, criando uma fonte interactiva de aprendizagem que, por sua vez, motiva cada utilizador a alargar os seus próprios conhecimentos e aprofundar o seu estudo numa abordagem desafiante, envolvente e instantânea (Prensky, 2003). As seguintes vantagens têm sido relacionadas com a utilização de jogos educativos (Abt, 1987):

- Os jogos introduzem os utilizadores a problemas e à resolução dos mesmos. Os jogos podem ser utilizados para motivar os alunos a envolverem-se em processos educativos, encorajando-os a criar e a colaborar.
- Os jogos têm objetivos claros. Quando cuidadosamente concebidos, os objetivos dos jogos podem ser ligados a objetivos educativos, contribuindo para a realização educacional.
- Através da visualização, os jogos contribuem para uma melhor compreensão de conceitos abstractos.
- Os jogadores assumem papéis realistas, concebem estratégias, e tomam decisões. Isto contribui para o desenvolvimento de pensamento crítico e analítico, bem como de capacidades de resolução de problemas.
- Os jogos fornecem feedback em tempo real. Isto facilita a compreensão das consequências das suas escolhas, descobrindo as ligações entre causa e efeito. Este processo contribui para a retenção do conhecimento.
- Os jogos também podem ser utilizados para a avaliação das consequências por parte dos alunos num ambiente seguro. Podem também ser utilizados em avaliações autênticas, ou seja, processos que simulam a forma como serão utilizados em contextos da vida real.
- Os jogos são benéficos e eficazes para formações (iniciais) que abrangem processos e práticas perigosas ou se a implantação de espaços físicos para formação for dispendiosa.

4.2 Salas de Fuga Educacionais

Uma "sala de fuga" é um jogo em que uma equipa de jogadores descobre pistas, resolve puzzles e realiza tarefas numa ou mais salas para alcançar um objetivo de vitória num período de tempo limitado. Os jogos são realizados numa variedade de locais fictícios, tais como celas de prisão, masmorras, laboratórios e até estações espaciais, dependendo do tema do jogo. Os objetivos dos jogadores e os desafios que encontram estão também alinhados com esse tema.
"O desenvolvimento de salas de fuga data de 2007 no Japão, onde foram implementadas para fins comerciais. Desde que foi introduzido nos E.U.A. em 2013, têm experimentado um rápido crescimento em popularidade (Nicholson, 2015)". (Martina, Richard & Göksen, Sultan, 2020)

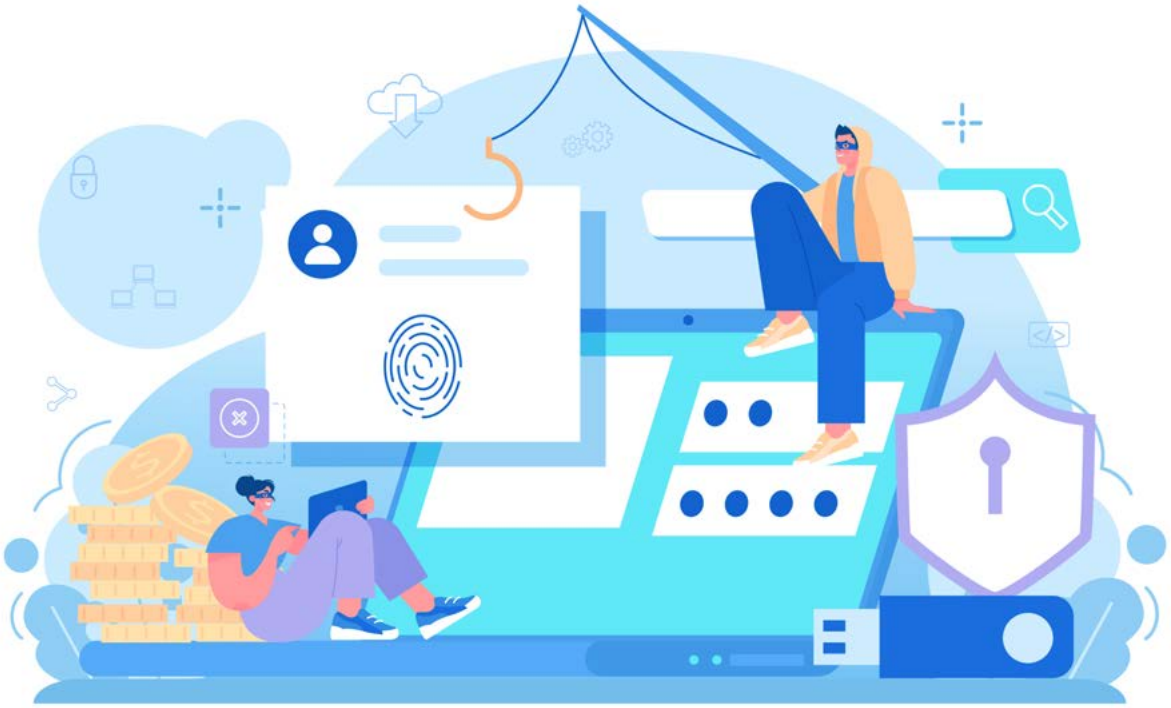
O jogo começa normalmente com uma breve introdução às regras do jogo, entregue sob a forma de vídeo, áudio, ou por um gamemaster ao vivo. Os jogadores entram, então, numa sala ou área onde se inicia um relógio que limita o tempo em que devem completar o jogo, que normalmente se situa entre 45 a 60 minutos. Os jogadores exploram então, encontram pistas, e resolvem puzzles que lhes permitem progredir mais no jogo. Estes desafios são geralmente mais mentais do que físicos, mas são necessários diferentes conhecimentos e capacidades para diferentes tipos de puzzles. Se os jogadores ficarem presos, pode haver um mecanismo pelo qual possam pedir dicas. As dicas podem ser dadas por escrito, vídeo ou áudio, ou por um gamemaster ao vivo. Os jogadores perdem se não forem capazes de completar todos os puzzles dentro do tempo previsto. Os bons finais são normalmente representados ou pela fuga "viva" dentro do tempo limite, completando o objetivo da sala, ou mesmo parando a ameaça ou antagonista da história, enquanto os maus finais representam normalmente os jogadores que são "mortos" pela principal força motriz da história ou um antagonista da sala que vem buscar os jogadores assim que o cronómetro se esgota. Além disso, o factor entretenimento nas salas de fuga também pode ser utilizado para encorajar a colaboração, o trabalho de equipa, e a formação de equipas.
As salas de fuga virtuais, digitais, ou online são equivalentes digitais de salas de fuga que se realizam através de um computador e de uma rede. A equipa comunica e colabora através de uma plataforma síncrona online como o Zoom enquanto utiliza uma aplicação de software que pode ser executada por um jogador e partilhada com os outros ou que permite o envolvimento de vários jogadores. Tal como nas salas de fuga física, as equipas resolvem enigmas e completam puzzles num período de tempo fixo. As salas de fuga digitais mais complexas podem utilizar a realidade virtual para aumentar a sensação de imersão dos jogadores.

Desde há vários anos, o sector académico também abraça os benefícios das Salas de Fuga e utiliza-as para os seus fins. Desde há algum tempo, existem vários estudos científicos sobre a eficácia e utilização das RCEs em todo o mundo. Na Europa, ainda não há demasiada investigação sobre o tema, mas está a crescer notavelmente (Tercanli, H. et al. 2021).

Os modelos de Salas de Fuga são utilizados em diferentes campos temáticos. O projeto EyesOnCS pretende apoiar a educação das PMEs em segurança cibernética, adoptando uma abordagem de sala de fuga num ambiente virtual. 22% das RCEs utilizadas até agora têm sido no campo da Informática e, portanto, já pertencem aos 3 principais estudos para os quais as RCEs já foram utilizadas (Tercanli, H. et al. 2021).
As Salas de Fuga Educativas são utilizadas para diferentes fases durante o processo de aprendizagem. Enquanto algumas RCEs não requerem qualquer conhecimento prévio e permitem aprender o básico, outras RCEs podem requerer conhecimento prévio e aprofundar o conhecimento com a sua abordagem pedagógica (Guckian et al. 2020; Mac Gregor, 2018; Tercanli, H. et al. 2022)

Em suma, ao utilizar a abordagem da Sala de Fuga, as competências transversais em geral são promovidas, mas também a motivação é aumentada e competências como a resolução de problemas, a formação de equipas, o pensamento fora de caixa e o questionamento crítico são trazidas para dentro. Para além das muitas competências diferentes, também é criada a consciência de um determinado tópico enquanto se aprende com a abordagem da Sala de Fuga. Assim, é um método de aprendizagem extremamente eficaz que aumenta significativamente o conhecimento dos participantes da Sala de Fuga em cerca de 53%. A consolidação do conhecimento também desempenha aqui um papel importante. (Tercanli, H. et al. 2021).
A abordagem do Modelo de Sala de Fuga também pode ser bem utilizada nas empresas. EyesOnCS e a Sala de Fuga resultante sobre segurança cibernética destinam-se a sensibilizar e formar os funcionários (não técnicos) no seu conhecimento do assunto. Aqui já começamos com o básico e assim damos aos jogadores uma sensação de segurança através de uma aprendizagem lúdica. Também aqui, como na IES, a curva de aprendizagem íngreme terá efeito e a motivação será dada para um tópico que ainda parece estranho a alguns.

5. Casos de Cibersegurança



A perspectiva da cibersegurança, especialmente para as PMEs, é preocupante. O nível de protecção das empresas não está relacionado com a inovação digitalizada em constante crescimento, nem com a interligação de dispositivos digitais. Muitas pessoas são também demasiado descuidadas na sua utilização privada de dispositivos finais e divulgam, impensadamente, informações privadas e pessoais na Internet. É importante mostrar os perigos e as consequências pessoais deste comportamento e explicar de forma adequada como lidar com a informação profissional. Uma vez que as pequenas e médias empresas garantem a estabilidade económica em muitos países europeus, é particularmente importante sensibilizar os trabalhadores para tornar a Europa um pouco mais resiliente.
É um objectivo importante deste compêndio proporcionar aos leitores experiências da prática da cibersegurança. Para alcançar este objectivo, os parceiros do projecto envolvidos compilaram diferentes incidentes de segurança. Estes casos de segurança são descritos em pormenor no capítulo seguinte.
Os casos foram recolhidos por todas as organizações parceiras em todos os países parceiros: Itália, Portugal, e Alemanha. Os capítulos seguintes fornecem uma descrição detalhada dos casos.

5.1 Casos italianos de cibersegurança

Caso 1 – A importância de firewalls na cibersegurança

Título	A importância de firewalls na cibersegurança
Origem do caso	Post e Italiane PST – Companhia Nacional de Correios (Itália)
Período de Ocorrência	Agosto 2021
Tags	Empresa, Roubo de Identidade, Ataque por e-mai, Phishing
Estado	encerrado até ao final de Agosto de 2021 por modificação das credenciais de login
Aplicabilidade Sala de Fuga	Altamente aplicável: É um caso comum que pode ser facilmente compreendido

Phishing:
Os ataques de phishing envolvem o envio em massa de e-mails fraudulentos a utilizadores insuspeitos, disfarçados de uma fonte fiável. Os e-mails fraudulentos têm frequentemente a aparência legítima, mas ligam o destinatário a um ficheiro ou script malicioso concebido para conceder aos atacantes acesso ao seu dispositivo para o controlar ou recolher reconhecimento, instalar scripts/files maliciosos, ou para extrair dados tais como informação do utilizador, informação financeira, e muito mais.
Os ataques de phishing podem também ter lugar através de redes sociais e outras comunidades on-line.[18]

Que tipo de ataque é?
Ataque de Phishing

Fraqueza/Vulnerabilidade:
Erro Humano- a falta de cautela ou ignorância da vítima levou à ameaça cibernética.

18 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

Figura 1: E-Mail.

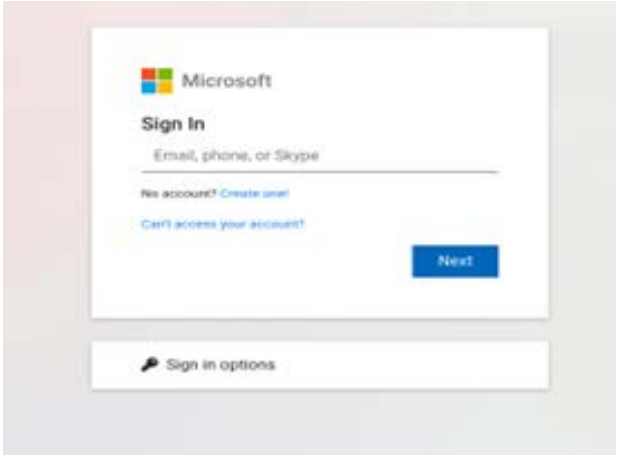


Figura 2: Iniciar sessão no Microsoft.

O que aconteceu?

- Cibercriminosos desconhecidos conseguiram localizar o contacto electrónico do funcionário, a vítima do ataque. A vítima recebeu um e-mail a pedir para actualizar as suas credenciais de login das equipas Office 365 (a plataforma online utilizada dentro da empresa).
- A vítima clicou no link falso incluído no correio enviado pelos cibercriminosos e introduziu a informação de login da conta da sua empresa.
- Como é que foi notado?
- A Equipa de Resposta de Emergência Informática (CERT) da empresa detectou poucos acessos suspeitos de outros países como Reino Unido, Argélia, Estados Unidos, enquanto a vítima fazia o logon a partir de Milão, Lombardia, Itália. Isto despertou a suspeita e desconfiança da CERT.

Que medidas foram adoptadas?

- CERT pediu à vítima que confirmasse se ele entrou na sua conta a partir desses países. A vítima negou, pelo que a CERT lhe pediu para alterar o seu login nas credenciais.
- Poste Italiane introduziu um sistema de monitorização eficaz que opera a nível nacional. Globalmente, o software de e-mail da empresa está equipado com um Firewall, nomeadamente um filtro de spam que intercepta e bloqueia a maioria dos e-mails maliciosos.

Qual é o resultado das medidas de defesa?

Quando qualquer um destes emails de spam consegue passar pelo filtro, os funcionários têm um botão na sua caixa de correio para reportar o email acima mencionado diretamente ao CERT. Uma vez que a CERT tenha analisado o correio eletrónico e o classifique como malicioso, extrai a informação e as ligações que contém e coloca-as em controlos perimetrais, bloqueando o acesso à ligação.

Caso 2 – Ataque à cadeia de abastecimento

Título	Ataque à cadeia de abastecimento
Origem do caso	ERG Evolving Energies - Companhia energética italiano
Período de Ocorrência	Agosto 2021
Tags	Empresa, Ataque ao servidor, Roubo de dados, Malware, Ransomware
Estado	fechado na semana seguinte à ocorrência por modificação das credenciais de login
Aplicabilidade Sala de Fuga	Não aplicável: As informações divulgadas pelo ERG sobre a forma como os peritos em SC agiram no tratamento do ataque de hacking não são detalhadas. Por conseguinte, seria difícil criar a narrativa do caso, especialmente porque faltam os principais aspectos técnicos do ataque.

Ransomware:
Um ataque Ramsomware é um malware que emprega encriptação para reter a informação de uma vítima no resgate. Os dados críticos de um utilizador ou organização são codificados para que não possam aceder a ficheiros, bases de dados, ou aplicações. É então exigido um resgate para fornecer acesso.
No caso de Ransomwares, as empresas têm opções limitadas

- pagar o resgate
- decifrar os dados roubados
- perder/ revelar publicamente os dados roubados.

Que tipo de ataque é?
Ransomware

Fraqueza/Vulnerabilidade:
No caso da Ransomwares, não é possível identificar um "erro humano", porque se trata de ataques direccionados perpetrados contra empresas cujos sistemas de protecção têm sido monitorizados e estudados ao longo do tempo pelos infractores

O que aconteceu?

ERG é o principal operador italiano de energia eólica e está entre os dez maiores operadores em terra no mercado europeu. O grupo opera nos sectores da energia eólica, energia solar, energia hidroeléctrica e energia termoeléctrica de cogeração de alto rendimento. A ERG conta com a Engenharia Informática para os seus serviços de segurança informática.

- De acordo com a reconstrução dos eventos pela imprensa, a 30 de Julho de 2021, o grupo de resgate LockBit 2.0 atingiu a Engenharia Informática conseguindo infectar os seus servidores com um vírus que alegadamente tinha comprometido as credenciais de acesso a algumas das VPNs dos seus clientes, incluindo ERG's.
- A Engineering Ingegneria Informatica comunicou o ataque aos seus clientes e iniciou extensas auditorias, através das quais, na noite de 5 de Agosto, detectou a matriz e a extensão do ataque, bem como as empresas invadidas por sua vez. O ataque foi
- conduzido por uma operação de resgate conhecida como RansomEXX, que passou pela Engineering Ingegneria Informatica até chegar ao sistema informático da ERG.
- Assim que entraram no sistema, os ciber-criminosos copiaram uma parte dos ficheiros da empresa, procedendo à sua encriptação. Os criminosos chantagearam publicamente o ERG partilhando a mensagem abaixo na página inicial do website do ERG, ameaçando a empresa de vazar os dados roubados dentro de poucos dias se a empresa não pagasse um resgate. O principal objectivo dos ataques de hacking é de facto roubar dados como alavanca nas tentativas de extorsão.

Como foi notado?

Durante o ataque, o ERG sofreu algumas perturbações limitadas na sua infra-estrutura de tecnologia de informação e comunicação (TIC).

Que medidas foram tomadas?

Activação imediata dos procedimentos internos de cibersegurança: O ERG não partilhou informações detalhadas sobre as acções técnicas empreendidas para combater os danos causados pelo ataque. A única informação certa disponível é que a sociedade CS nomeada pelo ERG, Engineering Ingegneria Informatica, solicitou à empresa que alterasse as credenciais de login para as contas.
Posteriormente, o ERG confirmou que todas as instalações estavam em bom funcionamento e não tinham sofrido quaisquer interrupções, assegurando assim as operações comerciais. Para negar o acesso dos cibercriminosos aos dados da empresa, a Engineering Ingegneria Informatica convidou o ERG a efectuar alterações de senha nas contas apoiadas pelas suas equipas e a comunicar qualquer outra suspeita de uso inadequado das suas credenciais.

Qual é o resultado das medidas de defesa?

Devido à extensão limitada dos danos, o ERG recusou-se a pagar o resgate. De acordo com a declaração do ERG, os hackers tinham dados codificados considerados bastante irrelevantes.

Caso 3 – Recusa de Serviço (DoS) Ataque

Título	Recusa de Serviço (DoS) Ataque
Origem do caso	Empresa de Aluguer Online (Itália)
Período de Ocorrência	Outubro 2021
Tags	PME, Empresa, Roubo de Dados, Negação de Serviço (DOS)
Estado	fechou na semana seguinte à ocorrência, fechando a plataforma online e criando uma nova plataforma.
Aplicabilidade Sala de Fuga	Aplicável com dificuldades: embora se trate de um caso comum, as suas consequências não são perfeitamente replicáveis.

DoS:
Os ataques DOS funcionam através de sistemas de inundação, servidores e/ou redes com tráfego para sobrecarregar recursos e largura de banda. Este resultado está a tornar o sistema incapaz de processar e satisfazer pedidos legítimos. Para além dos ataques de negação de serviço (DoS), há também ataques distribuídos de negação de serviço (DDoS). Os ataques DoS saturam os recursos de um sistema com o objectivo de impedir a resposta a pedidos de serviço. Por outro lado, um ataque DDoS é lançado a partir de várias máquinas hospedeiras infectadas com o objectivo de conseguir a negação de serviço e de levar um sistema para fora de linha, abrindo assim o caminho para outro ataque entrar na rede/ambiente.[19]

Que tipo de ataque foi?
Negação do serviço(DoS)

Fraqueza/Vulnerabilidade
Erro Humano–O chefe da Empresa foi mal aconselhado.

O que aconteceu?
- Antes da ocorrência do problema, a empresa apresentada tinha confiado ocasionalmente na Sync Security (SS), uma empresa privada de cibersegurança especializada em proteção de dados, conformidade e continuidade de negócios. Quatro meses antes do ataque, a SS detectou na plataforma online "Shutdown" que a empresa em questão estava classificada entre as

19 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

primeiras 100 empresas mais vulneráveis a ciberataques.

- Plataformas como "Shutdown" reportam dados – recolhidos ao longo do tempo por aranhas web – indicando o tipo e o nível de vulnerabilidade dos domínios das empresas e explicando as formas como tais vulnerabilidades podem ser exploradas. Estas plataformas são facilmente acessíveis a todos, expondo assim ainda mais as empresas que estão classificadas entre as primeiras cem.
- Está de fato estatisticamente provado que sofreu um ataque cibernético nos primeiros 12 meses após a publicação de tais classificações. Uma vez que os ataques perpetrados com base nas informações divulgadas por estas plataformas não são visados (em ataques não visados, os atacantes atacam indiscriminadamente o maior número possível de dispositivos, serviços ou utilizadores. Não se preocupam com quem é a vítima, uma vez que haverá uma série de máquinas ou serviços com vulnerabilidades[20]), pelo que é possível às empresas defenderem-se contra ameaças cibernéticas e prevenir a perda económica ou de dados.
- O SOC (Security operation system) da Sync Security comunicou, por conseguinte, este risco ao chefe da empresa, embora tenha subestimado a questão e se tenha recusado a recorrer a medidas de defesa preventiva.
- Quatro meses mais tarde, o website da Empresa na secção de interacção com o cliente baseada na forma sofreu um primeiro DOS: os cibercriminosos desconhecidos, de um país europeu – não especificado –, conseguiram bloquear o website, impedindo assim a sua produtividade.

Como foi notado?

Em muito pouco tempo, os ataques tornaram-se mais direcionados e profundos, resultando no comprometimento tanto dos dados comerciais como dos dados pessoais dos clientes. Por conseguinte, o chefe da Empresa exigiu a intervenção de peritos da Sync Security.

Que medidas foram adoptadas?

A intervenção foi imediata: Os peritos da Sync Security puseram em prática medidas de contenção. Em 3-4 horas, o ataque tornou-se ainda mais agressivo, pelo que as medidas postas em prática já não eram suficientes para conter os danos.
Os peritos da Sync Security, mediante autorização do CEO da empresa, tomaram a decisão drástica de bloquear o acesso ao site aos utilizadores fora de Itália.
Entre o problema – um erro relacionado com o código do website – foi corrigido e as práticas Anti-DOS foram postas em prática. Além disso, nos dias seguintes, os peritos da Sync Security fizeram uso de uma plataforma para monitorizar a classificação IP de cada utilizador.

Qual é o resultado das medidas de defesa?

Encerrar o website e reabri-lo assim que a ameaça tiver sido neutralizada.
O encerramento do website do Google através da sociedade de hospedagem resultou no desaparecimento da empresa e da sua plataforma de aluguer dos navegadores. Por conseguinte, a empresa teve de realizar campanhas promocionais, atividades de marketing e DEM (Direct Email Marketing) que pesaram ainda mais no orçamento das perdas.

20 National Cyber security center, https://www.ncsc.gov.uk/information/how-cyber-attacks-work, accessed on Juanuary 20 2023

Lições Aprendidas:
Após esta experiência, a empresa decidiu investir 0,5% das receitas na Cibersegurança, celebrando um contrato com a Sync Security.

Caso 4 – Injeção SQL

Título	SQL injection
Origem do caso	Companhia de seguros (Itália)
Período de Ocorrência	Outubro 2021
Tags	PME, Empresa, Informação sobre pagamento Roubo, injeção SQL
Estado	encerrado no final de Novembro de 2021, após uma auditoria técnica.
Aplicabilidade Sala de Fuga	Não aplicável: As informações sobre como os peritos em CS agiram no tratamento do ataque de hacking não são detalhadas. Por conseguinte, seria difícil criar a narrativa do caso, especialmente porque se tratava de um falso alarme.

SQL:
Isto ocorre quando um atacante insere um código malicioso num servidor utilizando a linguagem de consulta do servidor (SQL) forçando o servidor a fornecer informação protegida. Este tipo de ataque envolve geralmente a submissão de código malicioso num comentário ou caixa de pesquisa de um website desprotegido. As práticas de codificação segura, tais como a utilização de instruções preparadas com consultas parametrizadas, são uma forma eficaz de prevenir injeções de SQL.
Quando um comando SQL utiliza um parâmetro em vez de inserir diretamente os valores, pode permitir que o backend execute consultas maliciosas. Além disso, o interpretador SQL utiliza o parâmetro apenas como dados, sem o executar como um código.[21]

Que tipo de ataque é?
Injeção SQL.

21 https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

Fraqueza/Vulnerabilidade

Erro humano: o utilizador do website produziu um relatório tecnicamente impreciso.

O que aconteceu?

Nos meses que antecederam o ataque, a agência de Cibersegurança nomeada pela empresa realizou vários testes de penetração para avaliar o nível de segurança do sistema da empresa. Embora estes testes de segurança tenham sido realizados exaustivamente durante dez dias em Novembro de 2021, enquanto a empresa estava a realizar uma promoção de vendas, recebeu um relatório de uma organização de consumidores, o que acabou por bloquear a campanha.

Como foi notado?

Um membro da organização de consumidores alegou ter perdido o seu dinheiro enquanto introduzia as suas informações de pagamento no website da empresa.

Que medidas foram adotadas?

- O advogado da empresa sugeriu ao chefe da empresa que retirasse o website da Internet. Pensou-se ser um caso de injeção de SQL, alegadamente um cibercriminoso inseriu um código malicioso no servidor da empresa utilizando a Server Query Language (SQL), forçando assim o servidor a fornecer informação protegida.
- O chefe da empresa exigiu uma explicação da Agência de Cibersegurança: como foi possível que, logo após um teste de penetração, a empresa tenha sofrido um ataque cibernético? Especialmente porque para este tipo de agências, os ciberataques como as injeções SQL são bastante fáceis de detectar.
- A Agência de Cibersegurança tomou medidas imediatas, conduzindo também - em privado - uma análise passiva sobre o relatório.
- O cliente que relatou ter perdido o seu dinheiro enquanto introduzia as suas informações de pagamento no website da empresa era um estudante de engenharia informática, que, tendo algum conhecimento sobre o assunto, foi enganado pelo facto de ter lido "injection" dentro do código fonte HTML do website da empresa, quando este é apenas uma característica da linguagem de programação Java.

Qual é o resultado das medidas de defesa?

- As análises estáticas do programa determinaram que o ataque nunca ocorreu. Portanto, o roubo sofrido pelo utilizador não estava relacionado com o website da empresa. Embora fosse improvável que um sistema que só recentemente tinha sido submetido a testes de pressão tivesse uma vulnerabilidade; isto tinha de ser verificado oficialmente por auditoria técnica.
- O facto de ter retirado o website do mercado estava a custar à empresa uma grande perda de receitas.

Lições Aprendidas:
Neste caso, há menos um erro, mas antes um mérito. A empresa - por muito pequena que seja - ao confiar a um Agente de Segurança Cibernética profissional a realização de testes de segurança, provou ser previdente. De facto, o investimento feito em segurança cibernética, ajudou a empresa a evitar o risco de uma grande perda de lucros. De facto, tendo tido profissionais em que confiar, o website da empresa foi colocado de novo em funcionamento imediatamente após o resultado da análise técnica realizada em poucas horas. Pelo contrário, sem prevenção, este relatório feito pelo utilizador, que acabou por se revelar inexato, teria custado à empresa três vezes mais em lucros perdidos, para além do custo da intervenção de emergência por especialistas da CS.

Caso 5 – Smishing

Título	Smishing
Origem do caso	Pequena empresa de retalho
Período de Ocorrência	ocorreu em Março 2021
Tags	Empresa, Roubo de identidade, ataque por SMS, Phishing, Smishing
Estado	encerrado até ao final de Março de 2021 por modificação das credenciais de login.
Aplicabilidade Sala de Fuga	Altamente aplicável: É um caso comum que pode ser facilmente compreendido e que pode ser transferido para o modelo da sala de fuga.

Phishing e Smishing:
Smishing é uma forma de phishing que utiliza telemóveis como plataforma de ataque. O criminoso executa o ataque com a intenção de recolher informações pessoais, incluindo números de seguros sociais e/ou de cartões de crédito. O Smishing é implementado através de mensagens de texto ou SMS, dando ao ataque o nome "SMiShing".
Quando os cibercriminosos "phish", enviam e-mails fraudulentos que procuram enganar o destinatário para que este clique numa ligação maliciosa. O Smishing utiliza simplesmente mensagens de texto em vez de e-mail. Na sua essência, estes cibercriminosos estão a tentar roubar os seus dados pessoais, que podem depois utilizar para cometer fraude ou outros crimes cibernéticos.

Que tipo de ataque é?
Smishing

Fraqueza/Vulnerabilidade
Erro humano - a vítima caiu numa armadilha. Não se apercebeu que o seu banco já tinha os seus dados pessoais, pelo que não havia razão para pedir ao cliente que preenchesse um formulário. O cliente obviamente não sabia que um banco nunca pediria a um cliente para preencher formulários/logins via Email.

O que aconteceu?
- Os cibercriminosos desconhecidos conseguiram localizar o número pessoal do funcionário, a vítima do ataque. A vítima tinha solicitado a sub-rogação hipotecária, ou seja, tinha iniciado o processo de transferência da hipoteca de um banco para outro, no entanto, ainda estava à espera que o seu antigo banco lhe enviasse todos os documentos necessários.
- A vítima recebeu um SMS informando-o de que os seus documentos tinham sido carregados na sua conta bancária móvel e pedindo para clicar num link para proceder ao download a partir da área pessoal do website do banco. A vítima utilizou o computador da empresa para realizar este procedimento, para descarregar e imprimir os documentos no escritório. Ele clicou no link e foi redirecionado para um website, uma cópia perfeita do original, pelo que não se deu ao trabalho de verificar o URL do website. Aqui foi-lhe pedido para preencher um formulário com os seus dados pessoais: Nome, apelido, número de telefone, código fiscal.
- Uma vez feito, uma notificação "enviámos os seus documentos" apareceu, desta vez pedindo para clicar no link e inserir as suas credenciais de login. Embora a vítima estivesse certa de ter inserido as credenciais certas, no entanto a palavra-passe estava "errada". A página que aparentemente acabou de ser atualizada era a página real do Banco.
- Os criminosos roubaram as credenciais de início de sessão do Banco e, portanto, tiveram acesso aos dados pessoais da vítima. Utilizaram as credenciais e conseguiram ultrapassar o sistema de autenticação multi-factor, permitindo-lhes controlar o dispositivo token móvel e autorizar transferências bancárias diretamente da área pessoal do website do banco.

Como foi notado?
Após algumas horas, quando a vítima entrou na aplicação móvel do banco com o seu smartphone, percebeu imediatamente que tinha um saldo de conta mais baixo.

Que medidas foram adotadas?
- A vítima alterou as credenciais de login e notificou a instituição bancária que foi vítima de uma campanha de phishing.
- Informou sobre o ataque também dentro da empresa. A empresa nomeou um especialista em cibersegurança para realizar uma análise profunda do sistema se algum dos links que a vítima clicou, descarregou malware ou qualquer outra ameaça para a base de dados da empresa. A análise técnica não detectou qualquer vírus: os dados da empresa eram seguros.

Qual o resultado das medidas de defesa?

A situação foi resolvida através da alteração das credenciais de login. No entanto, a vítima não foi capaz de recuperar o dinheiro. Deveria ter contactado o Banco para se certificar da veracidade desse SMS. Além disso, ele não deveria ter utilizado o computador da empresa para tratar dos seus assuntos pessoais, mesmo que fosse urgente. Neste caso, também tem de ser considerado o lado psicológico da situação: as hipotecas são assuntos sensíveis, pelo que também é compreensível que a vítima tenha sentido a necessidade de tratar da papelada assim que recebeu o SMS - neste caso, um malicioso - a este respeito.

Caso 6 – Spam phishing

Título	Spam phishing
Origem do caso	Organismo governamental
Período de Ocorrência	ocorreu em 2018
Tags	Organismo governamental, Roubo de identidade, Engenharia social, Ataque por e-mail, Phishing
Estado	fechado por modificação das credenciais de login
Aplicabilidade Sala de Fuga	Aplicável com dificuldades: Esta é uma campanha de phishing muito sofisticada, pelo que seria difícil reproduzir certos elementos.

Engenharia Social:
A técnica de ataque de engenharia social consiste na manipulação psicológica para enganar os utilizadores a cometerem erros de segurança ou a darem informações sensíveis. Neste caso, os cibercriminosos desconhecidos investigaram primeiro as vítimas pretendidas, a fim de recolher informações necessárias, tais como potenciais pontos de entrada e fracos protocolos de segurança, necessários para prosseguir com o ataque.

Qu tipo de ataque é?

Spam phishing

Fraqueza/ Vulnerabilidade

Erro humano - Engenharia social. As vítimas caíram num esquema muito sofisticado, cuidadosamente detalhado e desenvolvido ao longo do tempo. Quando os cibercriminosos põem em prática processos para reter as vítimas, é muito difícil distinguir os e-mails maliciosos dos e-mails verdadeiros. Este é um dos maiores riscos associados à engenharia social, que alavanca as fraquezas das vítimas, neste caso uma recompensa psicológica ligada a uma paixão, para extorquir informação sensível.

O que aconteceu?

- No momento do ataque, os e-mails dos funcionários deste organismo governamental foram gerados da mesma forma: primeiro nome + apelido + domínio. Assim, a informação dos titulares dos endereços de correio electrónico não era obscurecida, uma vez que não eram considerados dados sensíveis.
- Isto tornou mais fácil para os criminosos localizar as identidades de um grupo de funcionários. Os perpetradores começaram a espiar os perfis sociais - Instagram, Facebook, Twitter, LinkedIn - destes funcionários, e ao olhar para as fotos e vídeos publicados, páginas seguidas, e seguidores, identificaram uma paixão comum de cerca de 20 funcionários: culturismo. Assim, iniciam uma campanha de phishing muito sofisticada.
- No início, os criminosos iniciaram uma atividade de teste de phishing: enviaram e-mails vazios às vítimas para verem quem mais provavelmente iria cair na armadilha. Posteriormente, estes funcionários receberam um e-mail relativo a um novo acordo entre o organismo governamental e uma famosa marca de suplementos de treino, ocasião em que esta marca estava a lançar uma campanha de vendas. Ao introduzirem as suas informações de compra e envio no link do e-mail, teriam aderido a esta campanha de vendas, recebendo os produtos à sua porta a um preço muito especial. Destes 20 empregados, apenas dois foram enganados.
- Ao clicar no link, foram redirecionados para a página de login - FAKE - do organismo governamental, onde "sendo uma promoção exclusivamente para os funcionários desse organismo governamental", foram obrigados a entrar com as suas credenciais de login: nome de utilizador e palavra-chave.
- Uma vez que o pagamento foi "finalizado" no website da marca FAKE - no qual até mesmo um número de serviço ao cliente estava disponível - os criminosos instauraram um processo para reter a vítima, enviando os bens adquiridos. Os criminosos certificaram-se de tornar o envio plausível: cuidando de todos os detalhes, tais como a embalagem, etiquetas, etc.
- Tendo recebido a mercadoria comprada, as duas vítimas espalharam a palavra entre os seus colegas sobre a alegada veracidade desta campanha de vendas. Assim, a ligação maliciosa resultante da campanha de phishing começou a circular entre os funcionários - a diferentes níveis - e em poucos dias cerca de 300 pessoas caíram na armadilha.

Como foi notado?

Só quando um superior soube o que se passava, sabendo que não havia qualquer acordo com esta marca, é que descobriu que o pessoal tinha sido vítima de um esquema. Os funcionários não só deram imprudentemente as suas informações pessoais e detalhes de pagamento, mas também expuseram em risco o corpo para o qual trabalham, o qual, como governo, possui um enorme número de dados pessoais dos cidadãos, cuja utilização para fins maliciosos poderia ser inumerável.

Que medidas foram adotadas?

- Para fechar as escotilhas, todas as contas das vítimas do golpe foram bloqueadas e as senhas foram posteriormente alteradas.
- O governo hoje passou a substituir também os nomes de utilizador.

Qual é o resultado das medidas técnicas / organizacionais / de defesa social?

- A situação foi resolvida através da alteração das palavras-passe e gradualmente dos nomes de utilizador.
- Hoje, quatro anos após o ataque, todos os endereços de correio eletrónico foram alterados: já não é possível rastrear a identidade dos titulares dos endereços de correio electrónico, uma vez que o nome e apelido foram substituídos por um código.

5.2 Casos de cibersegurança na Alemanha

Caso 1 – Spam E-mails

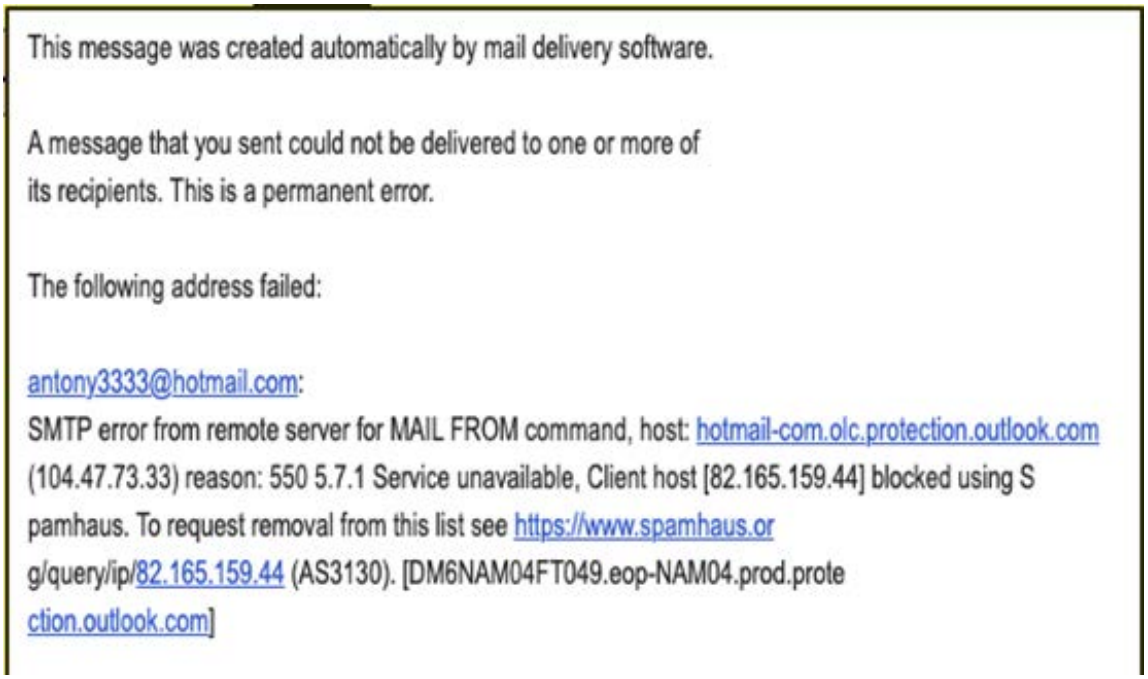
Título	Spam E-mails
Origem do caso	Consultoria em tecnologia de meios de comunicação, Alemanha/ PME local de Bielefeld
Período de Ocorrência	ocorreu em Março 2022
Tags	PME, Roubo de identidade, Email-attack, esquema
Estado	encerrado em 25.3.22 por modificação de senha
Aplicabilidade Sala de Fuga	Aplicabilidade e transferibilidade para o Modelo de Sala de Fuga Muito aplicável: O caso é fácil de ser compreendido e pode ser transferido para um modelo de sala de fuga limitada

Roubo de identidade:
O roubo de identidade é o crime de obter informação pessoal ou financeira de outra pessoa para utilizar a sua identidade para cometer fraude, tal como fazer transacções ou compras não autorizadas. O roubo de identidade é cometido de muitas formas diferentes e as suas vítimas são tipicamente deixadas com danos no seu crédito, finanças e reputação.

Que tipo de ataque é?
Roubo de identidade

Fraqueza/Vulnerabilidade:
Erro humano - Palavra-passe demasiado simples ou não alterada recentemente

O que aconteceu?
- O perpetrador aparentemente obteve a palavra-passe da conta da vítima. A partir desta conta, o cibercriminoso enviou e-mails de spam, presumivelmente em grande número para endereços desconhecidos da vítima.
- De acordo com a Figura 3, este correio foi bloqueado pelo servidor de recepção de correio com base na detecção de spam. Pode assumir-se que um elevado número de emails de spam enviados automaticamente da conta da vítima, chegou aos endereços especificados



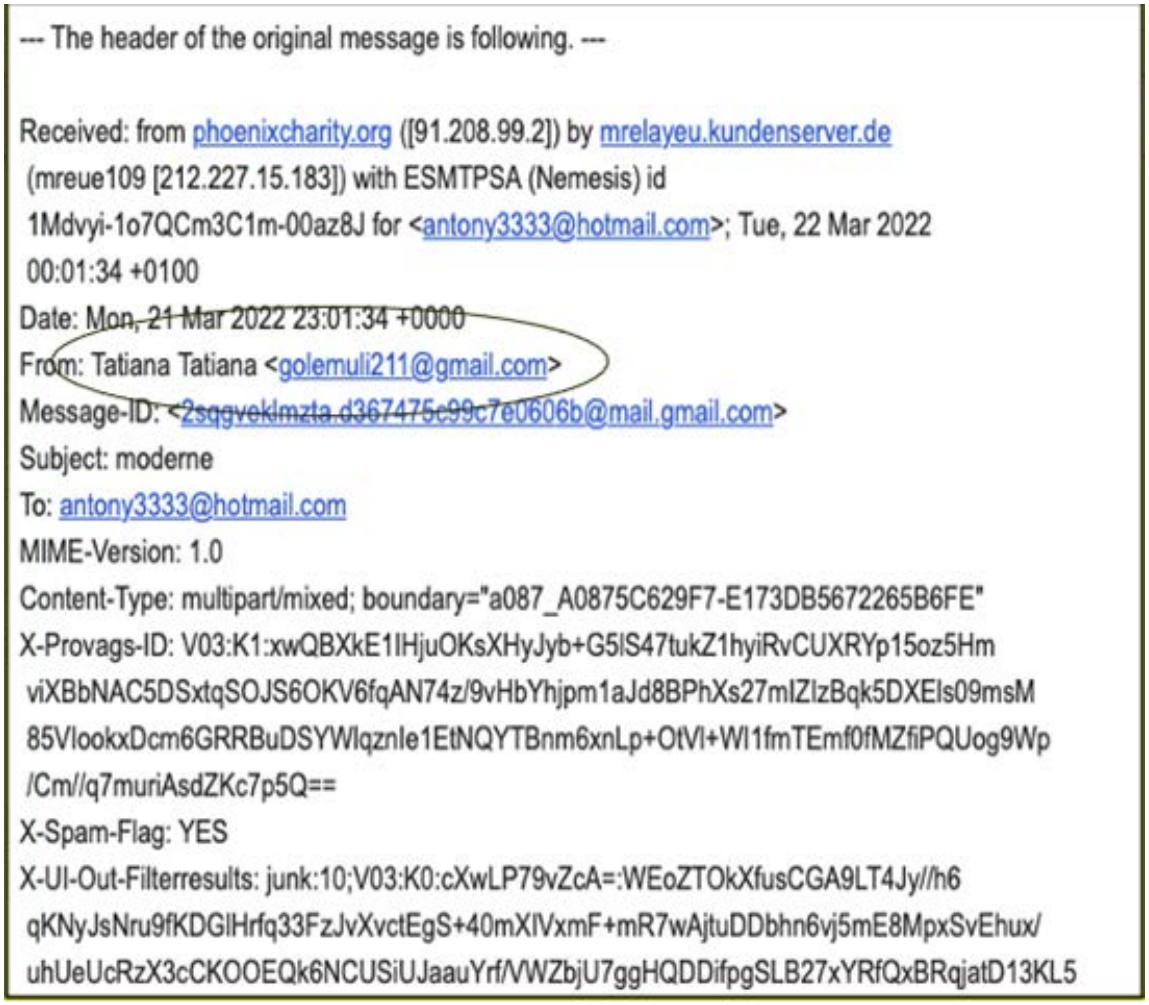
This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its recipients. This is a permanent error.

The following address failed:

antony3333@hotmail.com:
SMTP error from remote server for MAIL FROM command, host: hotmail-com.olc.protection.outlook.com (104.47.73.33) reason: 550 5.7.1 Service unavailable, Client host [82.165.159.44] blocked using S pamhaus. To request removal from this list see https://www.spamhaus.or g/query/ip/82.165.159.44 (AS3130). [DM6NAM04FT049.eop-NAM04.prod.prote ction.outlook.com]

Figura 3: Falha na entrega do e-mail no servidor do destinatário.



--- The header of the original message is following. ---

Received: from phoenixcharity.org ([91.208.99.2]) by mrelayeu.kundenserver.de (mreue109 [212.227.15.183]) with ESMTPSA (Nemesis) id 1Mdvyi-1o7QCm3C1m-00az8J for <antony3333@hotmail.com>; Tue, 22 Mar 2022 00:01:34 +0100
Date: Mon, 21 Mar 2022 23:01:34 +0000
From: Tatiana Tatiana <golemuli211@gmail.com>
Message-ID: <2sqgveklmzta.d367475c99c7e0606b@mail.gmail.com>
Subject: moderne
To: antony3333@hotmail.com
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="a087_A0875C629F7-E173DB5672265B6FE"
X-Provags-ID: V03:K1:xwQBXkE1lHjuOKsXHyJyb+G5lS47tukZ1hyiRvCUXRYp15oz5Hm viXBbNAC5DSxtqSOJS6OKV6fqAN74z/9vHbYhjpm1aJd8BPhXs27mlZlzBqk5DXEls09msM 85VlookxDcm6GRRBuDSYWlqznle1EtNQYTBnm6xnLp+OtVl+Wl1fmTEmf0fMZfiPQUog9Wp /Cm//q7muriAsdZKc7p5Q==
X-Spam-Flag: YES
X-UI-Out-Filterresults: junk:10;V03:K0:cXwLP79vZcA=:WEoZTOkXfusCGA9LT4Jy//h6 qKNyJsNru9fKDGlHrfq33FzJvXvctEgS+40mXlVxmF+mR7wAjtuDDbhn6vj5mE8MpxSvEhux/ uhUeUcRzX3cCKOOEQk6NCUSiUJaauYrf/VWZbjU7ggHQDDifpgSLB27xYRfQxBRqjatD13KL5

Figura 4: Cabeçalho do correio eletrónico não solicitado.

pelo atacante. Este é o principal impacto do ataque. Só se podem fazer suposições sobre o conteúdo enviado.
- Outras pesquisas[22] descobriram que frequentemente os e-mails de spam/scam com o endereço de retorno golemuli211@gmail.com distribuíam o conteúdo mostrado na Figura 4. Deve notar-se que o burlão não utilizou o endereço de retorno da vítima.
- Os danos parecem assim limitar-se ao envio de spam/scam a partir da conta da vítima. Não foi solicitado dinheiro à vítima.

Como foi notado?

O fornecedor de correio eletrónico da vítima reconheceu obviamente o abuso da conta e enviou o seguinte aviso à vítima (ver fig. 4). Ao mesmo tempo, a vítima do ataque reparou que as mensagens de correio eletrónico aparentemente enviadas da sua conta foram rejeitadas através da recepção de servidores de correio. O número destes e-mails era muito elevado, cerca de 200.

Que medidas foram adotadas?

Medidas: Mudança para uma palavra-chave mais segura
Para resolver o problema actual, realizámos as seguintes verificações e medidas:
- Verificação 1: O(s) e-mail(s) foi(foram) enviado(s) sem o conhecimento dos utilizadores?
  - Verifique os seus dispositivos finais (PC, smartphone ou tablet) com um verificador de vírus atualizado.
  - Atualizar o software nos dispositivos finais dos utilizadores e ativar as atualizações automáticas.
  - Utilize a firewall no seu router, PC ou software de segurança da Internet.
  - Se um vírus foi encontrado e removido com sucesso, altere as suas palavras-passe.
- Verificação 2: O utilizador enviou o correio de propósito?
  - Verifique se o software de correio eletrónico que está a utilizar está configurado corretamente.
- Verifique se os endereços dos destinatários são constatáveis, mantendo regularmente as listas de correio dos utilizadores.
- Se o utilizador enviar newsletters ou outros envios de correio electrónico em massa, teria sido tomada atenção às seguintes normas:
  - O remetente teve o consentimento do destinatário (opt-in duplo)
  - O boletim contém um link que permite ao destinatário cancelar a subscrição com apenas um clique (opt-out)
  - Os destinatários de correio electrónico para os quais o utilizador recebe uma mensagem não entregue são automaticamente eliminados da base de dados de endereços (bounce management)

Qual o resultado das medidas de segurança?

Neste caso, a senha de e-mail foi alterada pela vítima dentro de um curto período de tempo O bloqueio foi automaticamente removido pelo fornecedor em poucos minutos.

22 https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727

Caso 2 – Instalação do software Cripto Mineiro

Título	O software Crypto Miner foi instalado
Origem do caso	Cliente não revelado/ Alemanha
Período de Ocorrência	ocorreu Junho 2019
Tags	PME, mineiro criptográfico, roubo criptográfico, burla
Estado	fechado e tecnicamente resolvido
Aplicabilidade Sala de Fuga	Muito aplicável: O caso simples é fácil de ser compreendido

Mineiros criptométricos:
A extracção de moedas criptográficas é um processo de criação de novas "moedas" digitais. No entanto, isso é até onde vai a simplicidade. O processo de recuperação destas moedas exige a resolução de puzzles complexos, a validação de transacções em moeda criptográfica numa rede de cadeia de bloqueio e a sua adição a um livro-razão distribuído para a sua localização.

Que tipo de ataque é?
Mineiro criptográficos

Fraqueza/Vulnerabilidade:
Erro humano – Descarregar e instalar software de código aberto a partir da Internet foi o gatilho para este ataque. Não foi descarregado de sítios "seguros" ou "oficiais" dos fabricantes.

O que aconteceu?
- No site de um cliente, os mineiros criptográficos foram instalados como resultado de um download arbitrário de software por parte dos funcionários. Quando os mineiros criptográficos foram desinstalados, foi iniciada uma encriptação da estrutura da rede (servidores, clientes, backups, cópias sombra, etc.). Isto foi seguido de uma extorsão do cliente.

- Os funcionários do cliente tinham direitos de administração local e eram autorizados a instalar software nos clientes. Como resultado, os mineiros criptográficos também se tinham instalado.
- Os mineiros criptográficos começaram a trabalhar imediatamente após a instalação e utilizaram todos os recursos do cliente para a exploração mineira.

Como foi notado?

O desempenho dos clientes foi-se tornando cada vez pior. Processos simples demoraram muito tempo. Além disso, a utilização da CPU e da RAM foi consistentemente de 99%.

Que medidas foram adoptadas?

- A estrutura da rede foi desconectada da Internet
- Os clientes e servidores foram removidos da rede
- Toda a infra-estrutura técnica foi reinstalada
- Protecção uniforme contra vírus, backups armazenados externamente, direitos de administração foram retirados aos utilizadores
- Foi instalado um sistema de Firewall

Qual o resultado das medidas de defesa?

- Como resultado das medidas de segurança implementadas, não se verificou uma nova infestação.
- O malware que já tinha sido descarregado foi removido pelo sistema de proteção contra vírus antes de poder ser executado.
- Durante a desinstalação, o software iniciou uma encriptação da estrutura da rede. Aqui, todos os dispositivos disponíveis na rede foram encriptados.
- As cópias de segurança e cópias-sombra foram eliminadas e não puderam ser restauradas. O cliente foi reposto de 01.07.19 a 31.12.18.
- Os dados tinham de ser mantidos manualmente. Não houve resposta à extorsão.
- A infra-estrutura foi reinstalada e parcialmente restaurada a partir das antigas cópias de segurança existentes.

Lições aprendidas:
Este tipo de ataque pode acontecer novamente. Contudo, pode ser prevenido por uma protecção uniforme e atualizada contra vírus com módulos adicionais, tais como um Intercept X ou uma caixa de areia. Além disso, os direitos de administração podem ser retirados aos utilizadores, para que não se possa instalar apenas qualquer software.

Caso 3 – Ataque Phishing

Título	Ataque Phishing
Origem do caso	Cliente não revelado/ Alemanha
Período de Ocorrência	ocorreu em Fevereiro 2022
Tags	PME, phishing, fraude
Estado	O caso foi tecnicamente resolvido.
Aplicabilidade Sala de Fuga	Caso aplicável: O caso simples é fácil de ser compreendido e pode ser transferido para um modelo de sala de fuga limitada. Uma vez que o caso é um caso padrão muito frequente, não é muito interessante para o modelo.

Que tipo de ataque foi?
Phishing

Fraqueza/Vulnerabilidade:
Erro humano - o nome de utilizador e palavra-passe do cliente para a banca online foram introduzidos seguindo a ligação de um correio de phishing e transmitidos ao perpetrador de phishing.

O que aconteceu?
Foram enviados a um cliente e-mails de phishing com termos e condições atualizados ou alterações de custos. Posteriormente, teve de ser efectuado o login bancário online para visualizar as alterações.

Como foi notado?
O administrador de TI interno da empresa relatora foi contactado. Ele analisou e verificou o correio.

Que medidas foram adotadas?
- O domínio do correio foi bloqueado através da firewall.
- No entanto, cerca de 3000 euros foram transferidos para outra conta bancária por esta fraude. Atualmente, o reembolso através do banco ainda se encontra pendente.

Qual é o resultado das medidas técnicas / organizacionais / de defesa social?

- Foi realizada uma formação dos funcionários na área da sensibilização.
- Os funcionários receberam uma "folha de informação" com informações sobre como reconhecer os e-mails de phishing.
- Posteriormente, os e-mails de phishing deixaram de ser clicados e foram apagados diretamente.

Lições aprendidas:
Este tipo de ataque pode acontecer novamente em qualquer altura. Uma solução sustentável é difícil de implementar. Podem ser utilizados domínios oficiais de correio como o Gmail ou similares. Se os bloquear, entre outras coisas, os e-mails "oficiais/ corretos" deixarão de chegar. As ligações são também regeneradas cada vez que um ataque é perpetrado. Aqui o bloqueio apenas proporciona uma proteção temporária.

Caso 4 – E-mails/ataques de phishing

Título	Mails de phishing para obter dados de início de sessão de correio electrónico
Origem do caso	Administrador de um estabelecimento de ensino / Alemanha
Período de Ocorrência	ocorreu em Março 2022
Tags	PME, phishing, dados de início de sessão, spam
Estado	O caso foi processado e encerrado com êxito.
Aplicabilidade Sala de Fuga	Caso aplicável: O caso é simples e fácil de compreender e pode ser transferido para um modelo de Sala de Fuga limitado. Uma vez que se trata de um caso padrão muito frequente, não é muito interessante para o modelo.

Que tipo de ataque foi?

Phishing

Fraqueza/Vulnerabilidade:

Não houve qualquer comportamento incorrecto por parte do colega, que agiu correctamente e comunicou o incidente. Neste caso, a proteção contra spam e fraude permitiu que o correio

passasse, uma vez que a pontuação para uma defesa de correio não foi atingida.

Figura 5: Nota de segurança

O que aconteceu?

- O funcionário da instituição de ensino recebeu uma mensagem de correio electrónico de phishing dizendo que a sua palavra-passe de correio expirou e que deveria definir uma nova palavra-passe.
- O remetente do correio electrónico era o alegado fornecedor: Ionos (1&1) support.

Como foi notado?

- Devido à atenção e informação do funcionário, o problema foi detectado e os colegas informaram proativamente o administrador do departamento de TI. Os funcionários estavam cientes do fato de que os vários fornecedores de serviços nunca enviaram e-mails com este conteúdo. As palavras-passe não expiram na instituição.
- Além disso, após uma inspeção mais atenta, foi possível identificar o remetente como não legítimo.

Que medidas foram tomadas?

- O colega reencaminhou o correio electrónico para o administrador informático.
- O departamento de TI começou então a tomar as medidas de segurança habituais:
- Em primeiro lugar, foi formulada uma entrada no centro de mensagens para avisar todos os outros colegas de que tinham ocorrido ataques de phishing num determinado momento.
- Paralelamente, o remetente foi bloqueado para que não houvesse comunicação em segundo plano (lista negra).

Qual foi o resultado das medidas de defesa?

- Uma vez que as vítimas e os departamentos de TI são praticamente impotentes contra este tipo de ataques de phishing e que não podem ser instalados mecanismos de defesa sustentáveis sem restringir visivelmente o utilizador, não foi possível tomar outras medidas.
- Não houve danos, excepto o tempo de trabalho investido no esclarecimento do incidente.

Lições aprendidas:
Após a avaliação do incidente, foram planeadas campanhas preventivas adicionais e formação dos funcionários para aumentar o nível de alerta.

Caso 5 – Código malicioso em anexo de correio electrónico

Título	Código malicioso em anexo de correio electrónico
Origem do caso	Universidade / Alemanha
Período de Ocorrência	ocorrido em Junho 2016
Tags	PME, correio, anexo, spam, ransomware
Estado	O caso foi processado e encerrado com êxito.
Aplicabilidade Sala de Fuga	Caso muito bem aplicado: O caso é simples, mas instrutivo e fácil de compreender e pode muito bem ser transferido para um modelo interessante de sala de fuga. Para além disso, é possível desenvolver um cenário para uma história instrutiva e emocionante a partir do caso.

Ataque do Locky:
O Locky é um tipo de ransomware. Foi lançado em 2016 e os especialistas em segurança descobriram que os autores do malware entregaram este ransomware por correio electrónico, pedindo o pagamento através de uma factura anexada a um documento malicioso do Microsoft Word que executa macros infecciosas. O Locky Ransomware é uma peça de malware que encripta ficheiros importantes no seu computador, tornando-os inacessíveis e inutilizáveis. Mantém-nos 'reféns' e, entretanto, exige o pagamento de um resgate, em troca dos ficheiros encriptados.

Que tipo de ataque foi?
Ataque Locky - Ransomware Trojan.

Fraqueza/Vulnerabilidade:
Erro humano - Abertura de um anexo de correio electrónico desconhecido. O ataque bem sucedido foi favorecido pelo descuido da vítima e pela variante de dia zero deste Trojan.

O que aconteceu?
- Um e-mail com um ficheiro zip que supostamente continha facturas foi enviado a um membro da equipa (a vítima).
- Este ficheiro zip estava encriptado, o que impossibilitava os sistemas antivírus de o analisarem.

- A palavra-passe para o ficheiro zip estava no texto do e-mail.
- A vítima abriu o ficheiro zip sem mais verificações, descomprimiu o ficheiro xlsm e abriu-o. Depois disso, a vítima fez a sua pausa para almoço.
- A protecção antivírus (Kaspersky) - a variante de dia zero deste Trojan - e a pausa para almoço do colega significaram que a aplicação teve tempo suficiente em segundo plano para comprometer todos os dados.

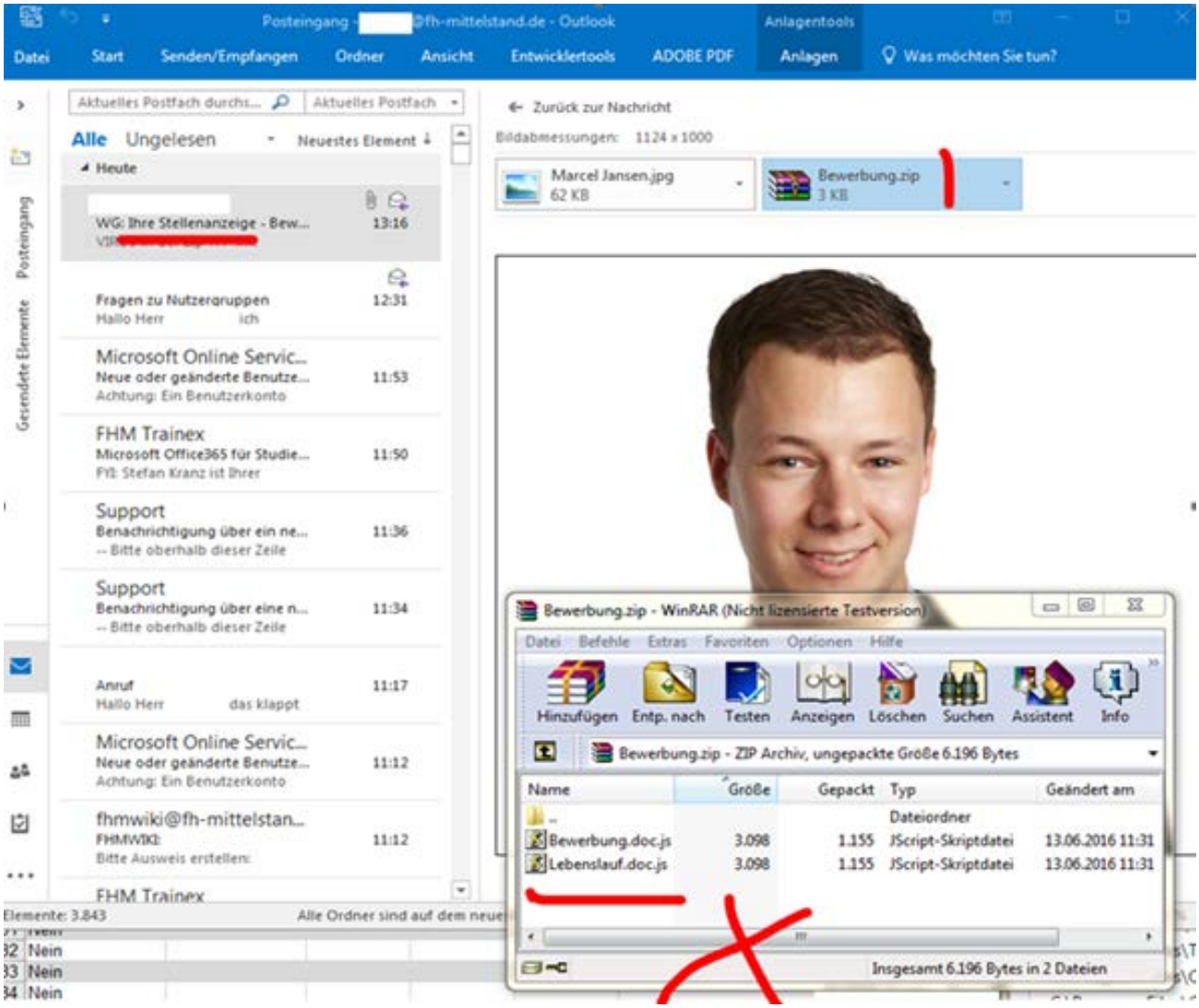


Figura 6: Anexo perigoso

Como foi notado?

- Quando a vítima regressou ao seu local de trabalho, questionou-se sobre a alteração do ecrã de fundo e informou o departamento de TI.
- Nessa altura, já tinha passado cerca de uma hora desde que a vítima tinha clicado no ficheiro macro-Excel anexado.

- No momento em que o administrador apareceu no computador da vítima para ajudar numa emergência, o administrador desligou imediatamente a LAN e desconectou a WLAN.
- Infelizmente, já era demasiado tarde e o ataque tinha sido executado com sucesso.
- O administrador encontrou uma situação catastrófica: todos os documentos estavam encriptados e já não podiam ser utilizados. Para além dos documentos locais, todos os documentos acessíveis nas unidades de rede também tinham sido encriptados.

Que medidas foram tomadas?

- Para iniciar a desencriptação, o criminoso exigiu 500 dólares sob a forma de Bitcoins.
- Como cerca de 50% dos membros da equipa já não conseguiam aceder aos documentos relacionados com o trabalho que se encontravam na unidade de rede.
- O administrador desmantelou então o portátil em questão. Ao mesmo tempo, foi publicado um aviso no Sistema de Gestão de Clientes (SGC) sobre este incidente, para que a acessibilidade telefónica pudesse ser restabelecida.
- O departamento de TI assegurou imediatamente que o computador portátil em causa deixasse de estar acessível na rede e que não fossem encriptados mais ficheiros na unidade de rede.
- O portátil foi completamente formatado e o Windows foi reinstalado. Não existiam ficheiros de trabalho locais.

Qual é o resultado das medidas de defesa técnica / organizacional / social?

- O departamento de TI, em consulta com a direção, importou uma cópia de segurança completa do dia anterior. Como resultado, todos os processos de todos os funcionários das últimas 24 horas deixaram de estar disponíveis. Para alguns funcionários esta situação foi muito crítica, mas para a maioria os danos foram limitados.
- A vítima recebeu uma formação especial para evitar que este caso se repetisse.
- Um dia mais tarde, foi recebida informação do fornecedor de antivírus da altura de que as ameaças Locky também tinham sido detectadas e evitadas.

Caso 6 – Fraude CEO

Título	Fraude CEO
Origem do caso	Universidade / Alemanha
Período de Ocorrência	ocorreu em Abril 2020
Tags	PME, correio, fraude, spam, burla
Estado	O problema continua a existir. (Pelo menos tentativas semelhantes continuam a ser detectadas, mas estão agora limitadas a um número limitado de exemplos, por exemplo, cartões de oferta da Apple).
Aplicabilidade Sala de Fuga	O caso é bem aplicável: O caso é simples, mas instrutivo e fácil de compreender e pode muito bem ser transferido para um modelo interessante de escape room. Além disso, é possível desenvolver um cenário para uma história instrutiva e emocionante a partir do caso.

Fraude do tipo " CEO":
O atacante afirma ser o CEO de uma determinada empresa e tenta forçar a vítima a realizar acções maliciosas e/ou fraudes em nome do verdadeiro CEO.

Que tipo de ataque é?

A fraude do CEO é uma forma altamente direcionada de spear-phishing em que os atacantes pesquisam as potenciais vítimas e as suas empresas online, aprendendo tudo o que podem a partir do site da organização, bem como informações de sites de redes sociais como o LinkedIn, Facebook e Twitter. Normalmente, o atacante tem como objetivo enganá-lo para que transfira dinheiro para uma conta bancária pertencente ao atacante, para que envie informações confidenciais de RH ou para que revele outras informações sensíveis.

Fraqueza/Vulnerabilidade:

- Trata-se de uma fraude do diretor-geral. O remetente afirma pertencer à direção com a intenção de cometer uma fraude.
- A protecção contra spam/scam do fornecedor de correio electrónico falhou ou sinalizou a "fraude".

- O funcionário não recebeu formação para reconhecer imediatamente pedidos não legítimos. O funcionário era também muito novo na empresa e tinha pouco contacto com outros colegas devido ao Covid-19.

O que aconteceu?

- Uma mensagem de correio electrónico, supostamente da direcção, chega aos colegas: Foi solicitada uma transferência de dinheiro para um país estrangeiro.
- Não se trata de um correio automatizado; a pessoa contactada teria podido iniciar esta transferência.
- Como o endereço de correio electrónico real do atacante é difícil de reconhecer pelo destinatário, o utilizador não se apercebeu disso.

Como foi notado?

- Dado que a transferência de dinheiro obedece a regras específicas e a um mecanismo de controlo no interior da organização, a legitimidade da transferência não pôde ser confirmada. Rapidamente se tornou claro que se tratava de um caso de fraude.
- Se o utilizador tivesse passado o rato directamente sobre o endereço de correio electrónico, teria rapidamente percebido que se tratava de uma tentativa de fraude.

Que medidas foram tomadas?

- O ataque foi resolvido através do bloqueio da conta de correio electrónico do remetente (conta Gmail do atacante).
- O caso foi comunicado à polícia, mas o autor não foi identificado.

Qual o resultado das medidas de defesa?

Não é possível proteger-se de forma sustentável sem restringir demasiado o envio de correio, pelo que a protecção proactiva continua a ser reforçada.

Caso 7 – Backdoor in Software – Ataque de espionagem

Título	Backdoor in Software – Ataque de espionagem
Origem do caso	Ministro do Interior NRW/ Düsseldorf/Alemanha
Período de Ocorrência	Não divulgado
Tags	Ataque de espiões, backdoor
Estado	Resolvido
Aplicabilidade Sala de Fuga	Caso muito aplicável: O caso é interessante e fácil de compreender e pode muito bem ser transferido para um modelo interessante de sala de fuga. Além disso, é possível desenvolver um cenário para uma história instrutiva e emocionante a partir do caso.

Ataque de Espionagem
O roubo de resultados de investigação, de informações sobre o desenvolvimento de produtos, de números de balanços e de dados de clientes causa danos a longo prazo às empresas em causa: os concorrentes estrangeiros obtêm os dados gratuitamente. Pode perder-se uma vantagem competitiva duramente conquistada e as vendas de produtos diminuem
Os serviços de informações estrangeiros dispõem de excelentes competências informáticas e dissimulam o seu acesso. A descoberta de um ataque ocorre frequentemente apenas quando um informador externo alerta a empresa para o ataque.

Que tipo de ataque foi?
Ataque de espiões, backdoor

Fraqueza/Vulnerabilidade:
O software de terceiros não deveria ter sido utilizado sem controlo na rede da empresa. Em vez disso, deveria ter sido utilizado um conceito de segurança para testar se o software podia ser utilizado isoladamente.

O que aconteceu?
- As empresas com relações comerciais no estrangeiro são frequentemente obrigadas a utilizar determinado software, por exemplo, para o processamento de obrigações fiscais.

- Um software especial de backdoor foi instalado em vários computadores da empresa da vítima, que estava ligada em rede a nível mundial.
- Através de uma backdoor oculta, um atacante conseguiu aceder a documentos na rede da vítima.

Como foi notado?
No rescaldo da instalação, sabe-se que o software obrigatório contém uma backdoor para o serviço de informações estrangeiro.

Que medidas foram adotadas?
O sistema foi completamente reinstalado e a backdoor foi fechada.

Qual é o resultado das medidas de defesa técnica / organizacional / social?
Foram impedidos outros ataques.

Caso 8 – Engenharia social alargada - Ataque de espionagem

Título	Engenharia social alargada - Ataque de espionagem
Origem do caso	Ministro do Interior NRW/ Düsseldorf/Alemanha
Período de Ocorrência	Não divulgado
Tags	Ataque de espionagem, engenharia social
Estado	Resolvido
Aplicabilidade Sala de Fuga	O caso é muito bom e aplicável: O caso é interessante e fácil de compreender e pode muito bem ser transferido para um modelo interessante de sala de fuga. Para além disso, é possível desenvolver um cenário para uma história instrutiva e emocionante a partir do caso.

Que tipo de ataque foi?
Ataque de espionagem

Fraqueza/Vulnerabilidade::
Os atacantes sabem habilmente como criar na vítima o medo de perder uma boa oferta. Além disso, o contacto telefónico reduz a desconfiança em relação ao atacante. No entanto, o documento malicioso não deveria ter sido aberto na rede da empresa. Mais uma vez, a "fraqueza humana" é explorada.

O que aconteceu?

- Em muitas áreas de alta tecnologia, é comum as pessoas serem contactadas por recrutadores com ofertas de mudança de emprego.
- Quando um empregado de uma empresa conhecida recebe uma chamada no seu telemóvel de um caçador de talentos, isso não parece fora do comum. Após uma breve conversa, o suposto agente anuncia que vai enviar uma oferta de emprego lucrativa. Pouco tempo depois, o documento chega à conta de WhatsApp do trabalhador. Quando ele tenta abri-lo no telemóvel, o processo é interrompido com uma mensagem de erro.
- No dia seguinte, o caçador de talentos volta a contactar o trabalhador e promete-lhe um potencial de ganhos excepcional com condições de trabalho atractivas. No entanto, é necessário dar imediatamente feedback sobre o interesse na oferta apresentada. Sem mais demoras, o empregado transfere o documento recebido na apresentação para a sua conta de correio electrónico profissional. Após uma breve confirmação para utilizar um modelo de formato especial, pode abrir o ficheiro no computador da empresa. Uma vez que a oferta não corresponde às suas expectativas, cancela o trabalho com o head-hunter. Depois disso, o processo é esquecido.
- Mais tarde, verifica-se que, ao abrir o documento, foi estabelecido um acesso remoto ao PC da empresa do empregado. Este acesso permitiu que os atacantes se espalhassem ainda mais na rede da empresa e divulgassem dados sensíveis. O roubo de dados só foi detectado quando os atacantes já tinham desaparecido há muito tempo.

Como foi notado?

Não há mais informações, porque o caso não foi divulgado pelo Ministério do Interior NRW.

What measures were taken?

Não há mais informações, porque o caso não foi divulgado pelo Ministério do Interior NRW.

Qual é o resultado das medidas de segurança?

Não há mais informações, porque o caso não foi divulgado pelo Ministério do Interior NRW.

Caso 9 – E-mail Phishing

Título	E-mail Phishing
Origem do caso	Nova Empresa de TI, Alemanha
Período de Ocorrência	Ocorreu em Maio, 2019
Tags	Empresa, phishing, ataque por correio electrónico, ransomware
Estado	O estado deste caso é o seguinte: encerrado no prazo de várias semanas após a ocorrência do problema, através da criação de uma nova rede e da substituição de todos os computadores ligados à rede durante o ataque.
Aplicabilidade Sala de Fuga	Altamente aplicável: Os emotet e os trojans são vulgarmente conhecidos, bem como o phishing.

Phishing
Já descrevemos os ataques de phishing, mas é importante notar que os ataques de phishing se adaptaram ao longo dos anos e estão a tornar-se cada vez "melhores" e mais sofisticados. Por isso, é importante manter-se atualizado sobre os métodos de phishing mais recentes...

Que tipo de ataque foi?
Ataque de Phishing

Fraqueza/Vulnerabilidade:
O funcionário activou macros para o ficheiro infectado.

O que aconteceu?
- Um funcionário abriu uma mensagem de correio electrónico de um remetente falso que se fazia passar por um parceiro de negócios. A mensagem de correio electrónico continha um documento Word infectado.
- Quando o funcionário abriu este ficheiro, apareceu uma mensagem de erro que lhe pedia para "activar" a edição.
- O empregado clicou nesta mensagem e o Emotet infectou o seu sistema e começou a espalhar-se pela rede.

Como foi notado?

Foram detectadas várias infecções e foram encontrados vários computadores infectados na rede.

Que medidas foram adotadas?

- Foram estabelecidas ligações de vários computadores ao exterior.
- O vírus foi removido com o Avira e o Windows Defender.
- Posteriormente, os administradores tentaram impedir que o malware comunicasse com a infra-estrutura da Emotet. Como não funcionou como pretendido, toda a rede foi desligada da Internet.
- Foram contactados prestadores de serviços externos e várias empresas de análise forense de TI.

Qual foi o resultado das medidas de defesa?

- Toda a intranet foi restaurada e todos os computadores que estavam ligados à intranet durante o ataque foram substituídos.
- O conceito de segurança foi revisto para evitar este caso no futuro.

Caso 10 – Chantagista Correio de phishing

Título	Chantagista Correio de phishing
Origem do caso	Grossista de material eléctrico (Alemanha)
Período de Ocorrência	Ocorreu em Fevereiro 2020
Tags	Empresa, phishing, ataque por correio electrónico, PME, ransomware
Estado	Encerrado no prazo de três semanas após a ocorrência do problema, mediante o pagamento do resgate.
Aplicabilidade Sala de Fuga	Altamente aplicável: A falta de cópias de segurança é um grande problema e a perda de dados sem uma cópia de segurança funcional é catastrófica.

Cópia de Segurança
Uma cópia de segurança é uma cópia de dados efectuada e armazenada separadamente dos dados originais. Esta cópia pode ser utilizada para restaurar os dados originais no caso de estes se perderem ou danificarem. É altamente recomendável criar e testar regularmente cópias de segurança numa empresa.

Que tipo de ataque foi?
Ataque de Phishing

Fraqueza/Vulnerabilidade:
A mensagem de correio electrónico infectada foi aberta inadvertidamente por um funcionário. O ransomware encriptou todos os ficheiros. A abertura negligente de e-mails e anexos suspeitos levou ao sucesso do ataque. Além disso, a empresa não tinha uma estratégia regular de cópias de segurança. A falta de controlo de cópias de segurança obrigou-os a pagar o resgate.

O que aconteceu?
- Um funcionário abriu um anexo de correio electrónico infectado. Todos os anúncios eram brancos e apresentavam um endereço de correio electrónico. A estirpe de malware Emoted infectou todos os computadores e, por conseguinte, encriptou todos os ficheiros ao seu alcance.
- Um fornecedor de serviços externo, a quem foi confiada a criação de cópias de segurança, ainda não as tinha criado. Não havia nenhuma cópia de segurança recente e as únicas disponíveis eram demasiado antigas para serem utilizadas.
- Ninguém supervisionava as cópias de segurança e verificava a data das últimas cópias de segurança. A comunicação com o prestador de serviços externo também não era regular.

Informações adicionais: As macros são frequentemente utilizadas em aplicações do Office, como o Word, o Excel e o PowerPoint. Estas macros são guardadas como parte do ficheiro do documento e são escritas numa linguagem de programação chamada VBA (Visual Basic for Applications). As macros podem ser utilizadas para infectar um sistema com malware.

Como foi notado?
Os ficheiros foram encriptados rapidamente e o sistema ficou inutilizável.

Que medidas foram adotadas?
- A empresa contactou a polícia e o chantagista.
- O chantagista exigiu 21 Bitcoins. Sem uma cópia de segurança funcional, a sua própria existência estava em risco. Por conseguinte, o resgate de 120 000 euros foi pago e todos os sistemas foram desencriptados.
- Comunicação por correio e ausência de facturação digital durante três semanas, o que resultou em enormes perdas financeiras.

Informações adicionais: Nem todas as empresas que pagam o resgate recuperam os seus ficheiros desencriptados. Mesmo que recuperem os ficheiros, é necessário examinar todos os ficheiros para detectar malware oculto.

Qual o resultado das medidas de segurança?

- O sistema de correio electrónico foi então mudado para uma solução de nuvem da Microsoft.
- As cópias de segurança externas são agora criadas semanalmente.
- Foram ativados planos de segurança e cópias de segurança regulares.
- Formações em cibersegurança

Caso 11 – E-mail de phishing com malware

Título	E-mail de phishing com malware
Origem do caso	Empresa de segurança das máquinas (Alemanha)
Período de Ocorrência	Ocorreu em Maio 2020
Tags	empresa, phishing, ataque por correio electrónico, ransomware
Estado	Encerrado no prazo de duas semanas após o encerramento da intranet.
Aplicabilidade Sala de Fuga	Altamente aplicável: As mensagens de correio electrónico são perigosas, as indicações das autoridades públicas devem ser levadas a sério e verificadas

Malware
Malware, abreviatura de software malicioso, é qualquer software concebido para danificar ou explorar um sistema informático ou uma rede. Existem diferentes tipos de malware, incluindo vírus, worms, cavalos de Tróia, ransomware e spyware. Está frequentemente ligado e escondido noutros softwares ou ligações.

Que tipo de ataque foi?
Ataque de Phishing

Fraqueza/Vulnerabilidade:
Abertura negligente de um anexo de correio electrónico infectado. Os funcionários não receberam formação adequada para poderem detectar uma mensagem de correio electrónico suspeita.

O que aconteceu?
Email com software malicioso foi aberto.

Como foi notado?
- A empresa foi informada por uma autoridade pública (Landeskriminalamt) de um ciberataque iminente, utilizando mensagens de correio electrónico infectadas.
- A empresa verificou esta chamada e decidiu desligar a sua rede sete minutos após a chamada.

Que medidas foram adotadas?
- Desconexão da rede
- Exame e desinfecção de todos os sistemas da rede. Após a desconexão, o malware foi identificado. A produção foi interrompida.
- Cada computador teve de ser desinfectado individualmente.
- O servidor de substituição assegurou a comunicação por correio electrónico.
- Informações suplementares: a desinfecção individual de cada computador é muito dispendiosa em termos de tempo e de custos para a empresa / O ataque poderia ter sido evitado com uma formação adequada.

Qual é o resultado das medidas de defesa técnica / organizacional / social?
Duas semanas mais tarde, o sistema informático e a produção estavam novamente a funcionar.

Caso 12 – Ransomware e Phishing

Título	Ransomware and Phishing
Origem do caso	Fornecedor de serviços informáticos
Período de Ocorrência	Ocorreu em Outubro de 2021
Tags	empresa, PME, ransomware
Estado	Em curso, 95 % dos sistemas foram restabelecidos.
Aplicabilidade Sala de Fuga	Altamente aplicável: A recuperação após um ataque bem sucedido tem de ser treinada para ser rápida e eficiente.

DeepBlueMagic
O DeepBlueMagic é aparentemente originário da China. Tal como várias estirpes de ransomware no passado, encripta ficheiros utilizando ferramentas de encriptação comuns, como o Bitlocker e o BestCrypt, nas quais os utilizadores confiam e utilizam frequentemente para encriptação.

Que tipo de ataque foi?
Malware "DeepBlueMagic" instalado através de correio electrónico de phishing.

Fraqueza/Vulnerabilidade:
Abertura negligente de um anexo de correio electrónico infectado. Os funcionários não receberam formação adequada para poderem detectar uma mensagem de correio electrónico suspeita.

O que aconteceu?
- Os fornecedores das autoridades públicas foram atacados. Foi aberto um anexo de correio electrónico infeccioso contendo malware.
- Não foram roubados dados pessoais.

Como foi notado?
Os utilizadores receberam e-mails dos cibercriminosos a informar que os seus ficheiros estavam encriptados e não podiam ser utilizados.

Que medidas foram adotadas?

- O escritório administrativo regional teve de fechar.
- Todos os sistemas foram encerrados.
- Para além dos sistemas principais, 4000 dispositivos finais tiveram de ser analisados para detecção de malware.
- As cópias de segurança foram restauradas, mas a recuperação ainda está a decorrer.
- Não foi pago qualquer resgate.

Informações adicionais: Este exemplo mostra a importância de um sistema de cópia de segurança funcional. Mesmo após o ataque, foi possível restaurar os dados sem pagar o resgate. Não se esqueça: sem cópia de segurança, não há pena.

Qual foi o resultado das medidas da defesa?

No final de 2021, 95 % de todos os dados tinham sido restaurados.

Caso 13 – Software Malicioso

Título	Software Malicioso
Origem do caso	Investimento start-up (Germany)
Período de Ocorrência	Ocorreu em Outubro de 2021
Tags	empresa, PME, ransomware, engenharia social
Estado	Encerrado após alguns dias, fechando a vulnerabilidade explorada.
Aplicabilidade Sala de Fuga	Aplicável com dificuldades: A exploração de vulnerabilidades exige um certo nível de conhecimento ou devem ser muito fáceis de detectar. No entanto, requerem um conhecimento mais profundo das TI

Engenharia Social
A engenharia social é a utilização da manipulação psicológica para influenciar indivíduos ou grupos a divulgarem informações sensíveis ou a realizarem acções que podem ser prejudiciais para eles ou para a sua organização. Isto pode incluir tácticas como phishing, vishing (phishing por voz) e manipulação ao telefone. O objectivo é sempre o mesmo: enganar as pessoas para que forneçam informações confidenciais ou acesso a sistemas ou redes.

Que tipo de ataque foi?
Ataque de ransomware apoiado por chamadas telefónicas de engenharia social.

Fraqueza/Vulnerabilidade
Os dados roubados foram utilizados para apoiar e dar credibilidade a chamadas telefónicas de engenharia social.

O que aconteceu?
- Ataques de phishing que foram apoiados por chamadas telefónicas de engenharia social para os clientes.
- A vulnerabilidade do sistema informático não foi detectada a tempo.
- A vulnerabilidade do sistema foi utilizada para divulgar dados dos clientes.

Como foi notado?
Durante uma análise do sistema, a fuga de segurança/ataque foi rapidamente localizada.

Que medidas foram adotadas?
- Os clientes foram informados três dias depois.
- As autoridades foram informadas.
- A vulnerabilidade foi encerrada.

Informação Adicional: Se um utilizador tiver de alterar uma palavra-passe, recomenda-se que o departamento de TI adequado publique requisitos relativos a palavras-passe fortes.

Qual o resultado das medidas de defesa?
Depois de a vulnerabilidade ter sido resolvida, os clientes foram notificados e solicitados a alterar as suas palavras-passe.

Case 14 – Software malicioso na Empresa

Título	Software malicioso na Empresa
Origem do caso	Fabricante de máquinas industriais (Alemanha)
Período de Ocorrência	Ocorreu em Julho 2021
Tags	Empresa
Estado	Recuperado após alguns meses
Aplicabilidade Sala de Fuga	Aplicável com dificuldades: O caso foi muito elaborado e não foi de modo algum culpa da empresa - lição a retirar: por muito boa que seja a segurança, pode sempre haver um ataque.

Spoof mails
Uma mensagem de correio electrónico falsa é uma mensagem em que o endereço de correio electrónico do remetente e outras partes do cabeçalho da mensagem de correio electrónico foram alterados para parecer que a mensagem de correio electrónico teve origem numa fonte diferente. Isto é frequentemente utilizado em esquemas de phishing e outras formas de fraude, uma vez que pode fazer com que a mensagem de correio electrónico pareça mais legítima para o destinatário.

Que tipo de ataque é?
Ataque elaborado e planeado há muito tempo, utilizando um prestador de serviços do estrangeiro como entrada na empresa através de um e-mail de phishing e de um website falso.

Fraqueza/Vulnerabilidade
O prestador de serviços foi utilizado como um ponto fraco - embora a segurança informática e o pessoal da empresa estivessem bem preparados.

O que aconteceu?
Os piratas informáticos enviam um correio falso a um fornecedor de serviços no estrangeiro. O correio estava ligado a um website perfeitamente falso, para que o fornecedor de serviços não pudesse reconhecer a fraude.

Como foi notado?

O sistema foi completamente desligado / inutilizado e todos os ficheiros foram encriptados.

Que medidas foram adotadas?

- Todos os sistemas foram desligados.
- Todos os processos comerciais foram interrompidos.
- Tentativa de chantagem com o grupo.
- Foi contratado um fornecedor externo de cibersegurança para ajudar a restaurar os sistemas.

Informações adicionais: Mesmo que um sistema de segurança funcione bem e o pessoal tenha recebido formação adequada, é sempre possível ser vítima de pirataria informática. Infelizmente, não existe uma segurança a 100% contra ataques.

Qual é o resultado das medidas de defesa?

- Foi criado um grupo de trabalho. Estabelecimento de novos canais de comunicação com notícias diárias.
- As autoridades públicas foram notificadas.
- Foi dada prioridade a diferentes áreas de negócio.
- A infra-estrutura foi reconstruída e foram envolvidos serviços externos de consultoria e apoio informático.
- As cópias de segurança foram restauradas e a recuperação foi dividida em três categorias: vermelho (ainda infectado), laranja (em quarentena) e verde (dados limpos).

5.3 Casos de cibersegurança em Portugal

Caso 1 – Denial of Service in communication services

Título	Negação de serviço em serviços de comunicação
Origem do caso	Wikipedia[23], Diário de Notícias[24]
Período de Ocorrência	Ocorreu em Fevereiro 2021
Tags	Empresa, telecomunicações
Estado	Fechado
Aplicabilidade Sala de Fuga	O caso pode ser transferido para o modelo Escape room porque mostra a importância da cibersegurança para a sociedade. No entanto, a empresa não divulgou informações suficientes para fornecer um cenário para o jogo.

Que tipo de ataque foi?

A empresa e a polícia não revelaram muitas informações. Suspeita-se que um grupo altamente sofisticado de piratas informáticos tenha conduzido o ataque através da exploração de algumas falhas de segurança em software que não foi actualizado, mas a exploração utilizada não foi revelada. O objectivo do ataque era garantir que a empresa não pudesse fornecer os seus serviços de comunicação.

Fraqueza/Vulnerabilidade::

As deficiências resultaram da falta de actualização de todo o software que geria os serviços de comunicação. Não é claro se houve também alguma colaboração interna.

O que aconteceu?

Os piratas informáticos exploraram a vulnerabilidade do software para obter acesso aos servidores e sistemas de comunicação e provocar falhas na comunicação.

Como foi notado?

- Falta de dados móveis nas redes 3G e 4G.
- Falta de serviços de SMS, TV e Internet fixa para os clientes.

23 https://pt.wikipedia.org/wiki/Ciberataque_%C3%A0_Vodafone_Portugal
24 https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

- Falta de serviço vocal.
- Não foi possível contactar o 112 (número dos serviços de emergência).
- A SIBS [detentora da marca Multibanco] é cliente da Vodafone. A sua rede de ATM's era suportada na rede Vodafone. Alguns dos ATMs, por terem uma rede de interligação à rede de dados móveis, estiveram indisponíveis até cerca da meia-noite, portanto:
- As lojas não podiam vender os seus produtos em linha porque as ligações ao principal operador bancário não estavam a funcionar.
- Os clientes não podiam utilizar as caixas multibanco.
- Os clientes não podiam pagar nas lojas com cartões.

Que medidas foram adotadas?

Os serviços de emergência e de saúde foram reencaminhados para outras empresas de comunicações. A empresa teve de parar todos os sistemas e depois teve de voltar a utilizar sistemas de comunicação mais antigos. Depois, gradualmente, teve de verificar e reiniciar todos os sistemas afetados. Este processo demorou cerca de duas semanas.

Qual o resultado das medidas de defesa?

Os serviços não foram atacados desde o incidente, graças às novas medidas de segurança implementadas.

Erros e reações:

Esta quebra na Vodafone deveu-se ao trabalho de piratas informáticos que exploraram uma vulnerabilidade de software. As pessoas ficaram muito perturbadas e algumas começaram a entrar em pânico, porque não conseguiam contactar outras pessoas ou contactos de emergência como o 112, algumas empresas perderam muito dinheiro e as pessoas receavam que os hackers tivessem acesso a informações privadas. No entanto, o diretor executivo da Vodafone garantiu que não houve acesso a informações privadas. Desde então, a empresa reforçou as medidas de segurança.

Caso 2 – Phishing em clientes de lojas de retalho

Título	Phishing em clientes de lojas de retalho
Origem do caso	Diário de Notícias[25]
Período de Ocorrência	Ocorreu em Novembro 2019
Tags	Empresa
Estado	Fechado
Aplicabilidade Sala de Fuga	Facilmente transferível para o modelo de Sala de Fuga

Que tipo de ataque foi?
Ataque de phishing a clientes de uma grande loja de retalho.

Fraqueza/Vulnerabilidade:
A abordagem de engenharia social foi muito bem feita e aproveitou-se dos clientes desprevenidos.

O que aconteceu?
As pessoas receberam mensagens de texto falsas de alguém que se fazia passar por funcionários da loja Continente, pedindo informações pessoais. Algumas pessoas acreditaram nas mensagens e forneceram os seus dados pessoais aos piratas informáticos.

Como foi notado?
As pessoas começaram a ver artigos a serem comprados com o seu cartão e conta de loja de retalho.

Que medidas foram adotadas?
Os clientes foram informados e avisados do ataque. Os clientes afetados receberam novos cartões.

Qual o resultado da medida de defesa?
A campanha de informação evitou que um grande número de clientes fosse afetado.

25 https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

Erros e Reações:

Os clientes da loja de retalho (Continente) foram vítimas de phishing e não verificaram a veracidade da informação contida nas mensagens de correio electrónico.

Caso 3 – Dados roubados de entidades públicas

Título	Dados roubados de entidades públicas
Origem do caso	RTP NOTICIAS[26]
Período de Ocorrência	Ocorreu entre Maio e Dezembro de 2017
Tags	Empresas, instituições públicas, pessoas singulares.
Estado	Fechado
Aplicabilidade Sala de Fuga	O caso pode ser transferido para o modelo Escape room porque: • É um caso relevante a ser explorado, especialmente devido ao seu amplo impacto e ao elevado perfil das vítimas (que poderia ter levado a consequências graves e à partilha de informações confidenciais). • Temos informações sobre os aspetos técnicos do ataque (as palavras-passe foram roubadas através de registos em canais de redes sociais, e os dados foram publicados em duas listas online - "Exploit.in" e "Anti Public" -, que circulam na dark web. • Podemos dividir a narrativa em diferentes momentos: desde quando foi dado o primeiro sinal de alerta e partilhados os primeiros dados (por volta de 2016) até quando foram encontradas as listas finais e o ataque foi tornado público

.

Que tipo de ataque foi?

Os piratas informáticos exploraram vulnerabilidades de software em servidores de instituições públicas que não eram mantidos de forma adequada do ponto de vista da cibersegurança

26 https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761

Fraqueza/Vulnerabilidade

Vários erros importantes que podem ser destacados nesta situação são:

- as pessoas utilizaram endereços de correio eletrónico profissionais e oficiais para se registarem em canais de redes sociais e outras plataformas,
- não foram tomadas medidas após o evento para proteger as contas reveladas (por exemplo, alterando as palavras-passe expostas).

O que aconteceu?

- Segundo a fonte, um documento com 20.416 páginas (com um total de quase 32,5 milhões de passwords) estava a circular na Internet, revelando dados pertencentes a funcionários e representantes de quase todas as áreas da administração pública, como ministérios, forças armadas, forças de segurança pública, administração fiscal e comissão nacional de eleições.
- As vítimas eram múltiplas e diversificadas: entidades públicas, grandes empresas, organismos governamentais, funcionários públicos e equipas de futebol.
- Além disso, foram também reveladas palavras-passe e e-mails de pessoas que trabalham em locais privados e públicos, como bancos, hospitais e meios de comunicação social. De acordo com as informações reveladas na altura, os dados pessoais dos utilizadores já estavam a ser roubados há anos antes de serem publicados e os hackers tinham-nos recolhido através de ataques a contas de redes sociais, como o Facebook, o LinkedIn, o Twitter, e a plataformas de armazenamento, como o Dropbox. Este ataque ficou conhecido como o maior ciberataque alguma vez registado em Portugal e o maior roubo de informação alguma vez registado.

Como foi notado?

No dia 20 de Dezembro de 2017, uma revista noticiosa portuguesa publicou um artigo que revelava que milhares de e-mails e palavras-passe tinham sido roubados por um grupo de hackers.

Que medidas foram adotadas?

- A polícia criminal iniciou imediatamente uma investigação sobre o ataque. No entanto, um representante das forças de segurança admitiu que a informação não era recente e que, de facto, já era conhecida há algum tempo (desde 2016).
- Após o evento, não foram tomadas medidas para proteger as contas reveladas (por exemplo, alterando as palavras-passe expostas).

Como foi o resultado das medidas de defesa?

Nesse sentido, e dado que muitas das palavras-passe reveladas ainda estavam activas cerca de um ano após a violação de dados[27], pode concluir-se que ainda existe uma falta de conhecimento sobre segurança em linha em várias instituições públicas e privadas portuguesas.

27 https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal

Caso 4 – Negação de serviço numa PME

Título	Negação de serviço numa PME
Origem do caso	Fonte interna
Período de Ocorrência	Ocorreu entre Janeiro e Fevereiro de 2022
Tags	PME
Estado	Fechado
Aplicabilidade Sala de Fuga	O caso pode ser transferido para o modelo Sala de Fuga porque mostra um problema simples que pode afetar a maioria das PME. Os aspectos técnicos do caso podem ser facilmente acedidos.

Que tipo de ataque foi?
Negação de serviço numa PME.

Fraqueza/Vulnerabilidade
A causa identificada foi um ataque à palavra-passe que permitiu capturar uma conta de correio electrónico dos funcionários que não utilizavam um esquema de geração de palavras-passe adequado.

O que aconteceu?
- Um ataque de palavra-passe que captura uma conta. Os piratas informáticos utilizaram essa conta para gerar mensagens de correio electrónico falsas.
- Algumas contas de correio electrónico e o servidor de correio electrónico estavam a ser utilizados para enviar spam para alguns endereços e causar Negação de Serviço. O domínio SME também foi colocado numa lista negra em alguns serviços.

Como foi notado?
O administrador do sistema começou a receber centenas de avisos sobre mensagens não enviadas ou enviadas para endereços errados. Em seguida, o fornecedor de serviços Internet contactou-o, alertando-o para a situação.

Que medidas foram adotadas?
O fornecedor de Internet que apoia a PME encerrou todos os acessos aos websites e ambientes em linha, exceto os utilizados para a administração. As palavras-passe foram alteradas e os ficheiros foram limpos. Foram adotados melhores esquemas de definição de palavras-passe.

Qual foi o resultado das medidas de defesa?
O arrombamento não se repetiu, embora os ataques continuem a ser frequentes

Case 5 – Code injection on websites

Título	Code injection on websites
Origem do caso	Internal Source
Período de Ocorrência	Occurred between October 2021 and March 2022
Tags	PME
Estado	The status of this case is closed
Aplicabilidade Sala de Fuga	The case might be transferred to the Escape room model because it shows a simple problem that can affect most SMEs. The technical aspects of the case can be easily accessed.

What kind of attack was it?
Software exploit of some WordPress plugins. Code was injected in those files.

Weaknesses/Vulnerability
SME staff was not using appropriate measures to protect forms on the websites.

What happened?
Hackers used unprotected forms in the hosted websites to:
- Inject code in some pages to install trojans.
- Execute software.
- Generate log registers entries to fill up disk space.

How has it been noticed?
The ISP runs regular security checks on the servers that detected the injected code.

What (technical) measures were taken?
Files were cleaned and all the plugins were updated.

What is the result of the technical / organizational / social defence measures?
There has not been a repetition of the break-in although attacks are still frequent.

Case 6 – Dados roubados de um clube de futebol

Título	Dados roubados de um clube de futebol
Origem do caso	Todos os meios de comunicação social em Portugal
Período de Ocorrência	Ocorreu entre 2018 e 2019
Tags	Empresa
Estado	Em tribunal
Aplicabilidade Sala de Fuga	O caso pode não ser transferido para o modelo de Sala de Fuga, porque os aspectos técnicos do caso não são facilmente acessíveis

Que tipo de ataque foi?

Não é claro se o cibercriminoso obteve acesso através de phishing ou de um ataque por palavra-passe.

Fraqueza/Vulnerabilidade:

Falta de medidas de segurança eficazes nos sistemas que eram utilizados por pessoas com poucas competências digitais.

O que aconteceu?

- Hackers tiveram acesso aos emails da direcção de um grande clube de futebol em Portugal.
- Um arquivo com vários terabytes de mensagens de correio electrónico foi então disponibilizado a um canal de notícias que as tornou públicas. Algumas das mensagens indicavam corrupção e suborno de diversos agentes desportivos por parte dos dirigentes do clube.

Como foi notado?

Um canal de notícias público recebeu a base de dados com as mensagens de correio electrónico e tornou-as públicas.

Que medidas foram adotadas?

O hacker responsável foi identificado e detido. O caso está atualmente a ser julgado. O clube afectado contratou uma nova solução para as suas necessidades de envio de mensagens.

Qual foi o resultado das medidas de defesa?

O clube deixou de estar dependente de técnicos internos de cibersegurança, que claramente não estavam à altura do desafio.

6 Conclusão

A maioria dos casos ilustrados neste compêndio afirma que o grau de proteção nas PME não está relacionado com a inovação e o progresso digitalizados em constante expansão. As fraquezas e vulnerabilidades persistem entre os funcionários que utilizam frequentemente dispositivos finais sem o devido cuidado e atenção à cibersegurança. Continua a verificar-se a falta de competências e de conhecimentos sobre as ciberameaças, bem como sobre a extensão dos possíveis danos para a empresa ou para o próprio indivíduo.

Os exemplos recolhidos em três países europeus revelaram que os problemas e desafios enfrentados pelas PME europeias são comparáveis. Esta semelhança permite a elaboração de soluções de colaboração para melhorar o estado atual. De um modo geral, é importante realçar os riscos e as repercussões individuais de comportamentos inalterados, incautos e desatentos, e fornecer orientações sobre como agir e reagir corretamente. Dado que as pequenas e médias empresas contribuem para a estabilidade económica em todos os países europeus, torna-se especialmente crucial sensibilizar os trabalhadores, contribuindo assim para a resiliência e a segurança digital da Europa.
A natureza e o tipo de vulnerabilidades são consistentes e comparáveis nas PME, abrangendo phishing, engenharia social, ransomware e palavras-passe inseguras. Uma parte significativa desses ataques pode ser atribuída a erros humanos. Muitas empresas aplicam abordagens semelhantes para combater os ataques e retificar a situação através da implementação de medidas de segurança técnicas e organizacionais.

No entanto, nem todos os líderes das PMEs interiorizaram de forma consistente as lições aprendidas. Em várias empresas, os líderes estabeleceram sistemas preventivos contra ciberataques e ameaças, e apenas algumas optaram pela formação do pessoal como medida de segurança subsequente. Esta opção parece ser, até à data, menos prioritária e menos frequentemente adoptada.
As reacções e respostas decorrentes dos ciberataques nas PME apresentadas revelam uma deficiência na compreensão e no reconhecimento da importância e do valor da educação e da formação nesta área. Estes resultados sublinham, mais uma vez, a necessidade premente de criar e proporcionar oportunidades e programas educativos destinados a atenuar as lacunas de competência entre o pessoal não técnico. Dotar as empresas e organizações de conhecimentos e competências essenciais é crucial para garantir operações de processos empresariais eficazes e seguras.

Este compêndio foi publicado para apoiar as PMEs a lidar com ataques de cibersegurança relevantes. O próprio projeto EyesOnCS pretende contribuir para a formação em cibersegurança dos funcionários das PME europeias e dos estudantes do ensino profissional.

7 Referências

- Abt, C., Serious Games (1987): University Press of America.
- Agrawal, S.; Simon, A.; Bech, S.; Bæntsen, K.; Forchhammer, S. (2020): Defining immersion. Literature review and implications for research on audiovisual experiences. J. Audio Eng. Soc., 68, 404–417.
- ACN Italy: National Cybersecurity Strategy 2022 – 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, seen 29.7.22.
- Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html , seen 28.7.22.
- Cyber security intelligence: National Cyber Security Centre Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html , seen 29.7.22.
- ENISA (2022): Consolidated Annual Activity Report 2021, Attiki, 2022.
- ENISA (2021): Cybersecurity for SMES- Challenges and Recommendations, European Union Agency for Cybersecurity (ENISA), Attiki, 2021.
- European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework , seen 29.7.22.
- EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 32019R0881 - EN - EUR-Lex , seen 28.7.22.
- EyesOnCS Projektteam (2023): Cyber Alert Scenario_0x_nn, Preliminary report of the project team, to be published, FHM Düren, Düren, 2023
- Guckian,. J., Sridhar, A. & Meggitt, S. J. (2020): Exploring the perspectives od dermatology undergraduades with an escape room game. Clinical and Experimental Dermatology, 45 (2), 153-158. https://doi.org/10.1111/ced.14039

- Juzeleniene, S., Mikelioniene, J., Escudeiro, P., Vaz de Carvalho, C. (2014): GABALL project. serious games-based language learning. Procedia-Soc. Behav. Sci. 136, 350–354.

- Mac Gregor, M. (2018). Campus Clue: Habituating Students to the Information Search Process via Gaming. Pennsylvania Libraries: Research & Practice, 6 (2), 86-92. https://doi.org/10.5195/palrap.2018.172

- Martina, Richard & Göksen, Sultan. (2020). Developing Educational Escape Rooms for Experiential Entrepreneurship Education. Entrepreneurship Education and Pedagogy. https://www.researchgate.net/publication/346548119_Developing_Educational_Escape_Rooms_for_Experiential_Entrepreneurship_Education , seen 10.1.23.

- Michael, D.R., Chen, S.L. (2006): Serious Games. Games That Educate, Train, and Inform. Thomson Course Technology PTR, Oshawa.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/ , seen 28.7.22.

- N.N.: About ENISA - The European Union Agency for Cybersecurity, https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity, seen 28.7.22.

- N.N.: https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727, seen 28.7.22

- N.N.: https://www.dn.pt/sociedade/servicos-de-voz-movel-da-vodafone-registam-recuperacao-progressiva-14568590.html , seen 28.7.22.

- N.N.: https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html, seen 28.7.22.

- N.N.: https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761, seen 28.7.22.

- N.N.: https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal/, seen 28.7.22.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/, seen 28.7.22.

- N.N.: Deutschland sicher im Netz, https://www.sicher-im-netz.de, seen 28.7.22.

- Oblinger, D. (2006): Simulations, games, and learning. ELI White Paper, vol. 1, no. 1.http://net.educause.edu/ir/library/pdf/ELI3004.pdf.

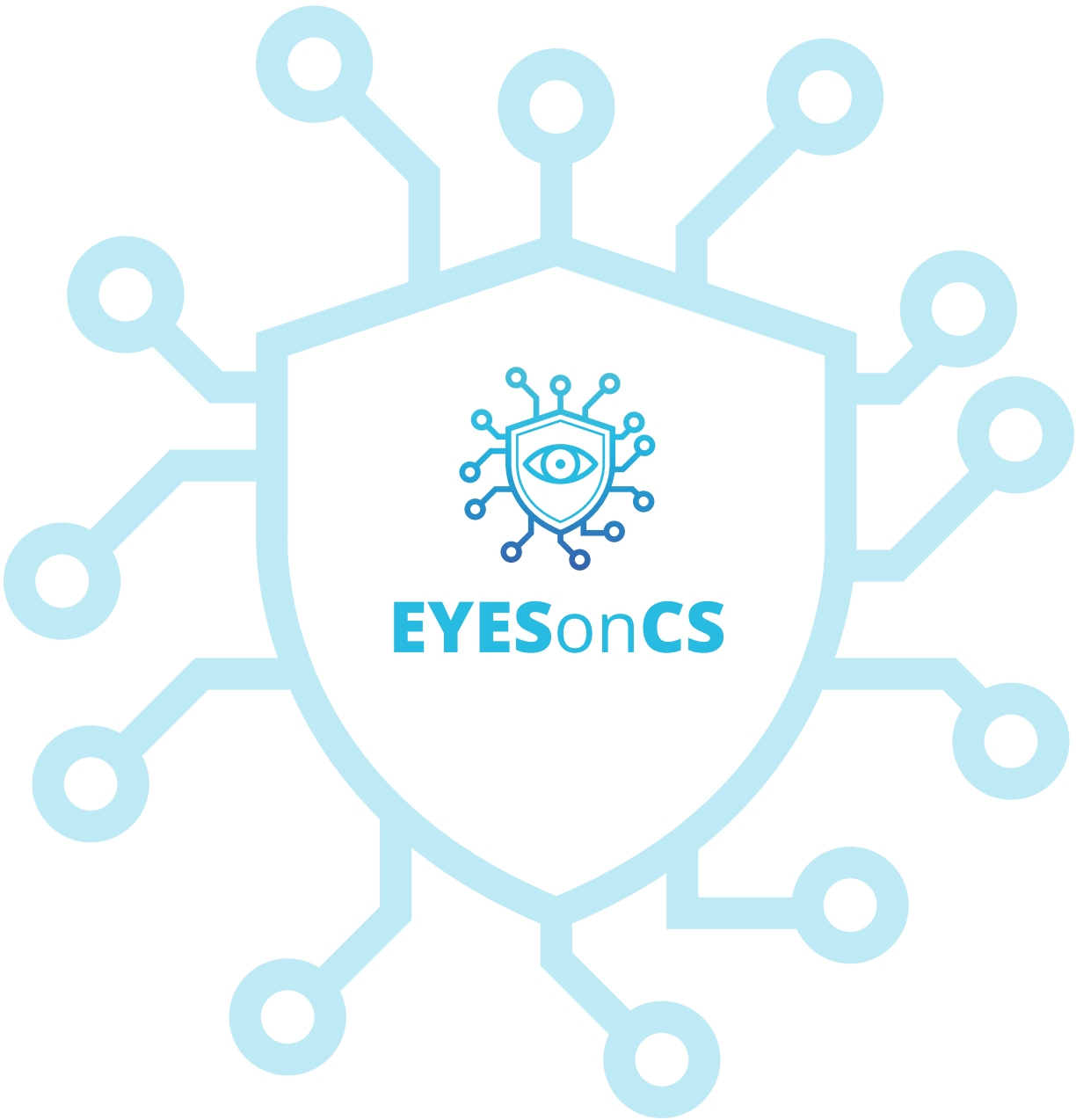
- Prensky, M.(2003): Digital Game-Based Learning. Comput. Entertain. (CIE) 1(1), 21 .

- Streim, A., Mann, S. (2021): Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, bitkom, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr , seen 2.3.23

- Tercanli, H., Martina, R., Ferreira Dias, M., Reuter, J., Amorim, M., Madaleno, M., Magueta, D., Vieira, E., Veloso C., Figueiredo, C., Vitòria, A., Wakkee, I., Gomes, I., Meireles, G., Daubariene, A., Daunoriene, A., Mortensen, A., Zinovyeva, A., Rivera-Trigueros, I., Lòpez-Alcarria, A., Rodrigìguez-Dìaz, P., Olvera-Lobo, M.D., Ruiz-Padillo, D.P., And Guitièrrez-Pèrez, J. (2021), Educational escape rooms in practice: Research, experiences and recommendations. UA Editoria. https://doi .org/10.34624/rpxk-hc61

- Zyda, M. (2005): From visual simulation to virtual reality to games. Computer 38(9), 25–32.

Notas



Fique atento!
Siga-nos e saiba mais
sobre o projeto em:

www.eyesoncs.eu

Cofinanciado pela
União Europeia