A cibersegurança e o panorama na sociedade

Gilberto Silva – 2222007

Lucas Ferreira – 2220862

Miguel Moreira – 2221090

Soraia Castro - 2220988

ISCAP (Portugal)

ISCAP (Portugal)

ISCAP (Portugal)

ISCAP (Portugal)

Resumo

Um dos principais desafios nas organizações modernas é a cibersegurança. Tendo em conta a digitalização e a crescente necessidade de dados atualizados, as ameaças da internet acabam por ser mais atuais e frequentes. Neste trabalho, iremos explorar a relação entre cibersegurança e gestão de informação, fazendo uma análise sobre como as organizações se podem prevenir de forma a manter a segurança dos dados e da informação.

Em primeiro lugar, abordaremos as ameaças possíveis, como *malwares*, *phishing* e *ransomwares*, daremos também destaque ao impacto que estas ameaças podem ter, tanto na integridade como na confidencialidade e disponibilização da informação. Em segundo, procuraremos encontrar as melhores práticas de cibersegurança, como por exemplo, a implementação de políticas, formação contínua dos colaboradores e o uso de tecnologias atuais como por exemplo criptografia e autenticação de dois fatores.

Por último, vamos apresentar um estudo sobre falhas na segurança de uma organização (estudo de caso fictício), fazendo análise às lições aprendidas e às estratégias utilizadas de forma a melhorar a segurança na instituição, com o objetivo de concluir que a cibersegurança é uma prioridade contínua para qualquer organização e é também extremamente necessária para manter uma gestão informacional eficaz e segura.

Palavras-chave: cibersegurança, gestão da informação, políticas da informação

INTRODUÇÃO

Atualmente, é possível perceber que o mundo está cada vez mais globalizado e digital, a cibersegurança revela ser um fator de grande importância no que se refere à salvaguarda dos direitos dos cidadãos e das propriedades intelectuais virtuais. De facto, a sociedade em geral,

que possui dispositivos eletrônicos e acesso à internet, está exposta a crimes cada vez mais elaborados que podem envolver roubo, extorsão e assédio. Estes crimes mais facilmente despercebidos, originaram a elaboração de políticas por parte da União Europeia o que influenciou o modo como este tema passou a ser tratado. A cibersegurança tem um significado abrangente, que pode ser classificado como:

O conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem. (Hermenegildo, 2020, p.1)

Além deste aspeto, a cibersegurança abrange a segurança do equipamento eletrónico e também pode ter atuações patrocinadas pelas leis que variam de país ou comunidade económicas como é o caso da União Europeia. A sociedade está intrinsecamente ligada à cibersegurança, já que a confiança nas autoridades, instituições e no sistema político no qual estamos inseridos, vai depender da resposta e das atitudes tomadas contra o cibercrime.

1 PANORAMA DA SOCIEDADE

Devido ao facto de vivermos em uma sociedade globalizada, com acesso à internet nos nossos aparelhos eletrónicos, como refere Dumit (2023, p.62) “O panorama do mundo cibernético tem evoluído numa frequência exponencial e com isso os recursos tecnológicos têm encontrado seu espaço no quotidiano das pessoas”. Foi necessário criar leis que fizessem cumprir as liberdades e os direitos de cada um de nós e assim atendessem a essa realidade, assim como estabelecimento de normas éticas e sociais de modo que os cidadãos fossem protegidos de eventuais ataques e crimes que pudessem acontecer como *malwares*, *phishing* ou *ransomwares*.

1.1 Malwares

Utilizados para fins maliciosos, os malwares são softwares que têm o objetivo de realizar a extração de informações relevantes como dados de cartão de crédito ou dados pessoais para depois ser realizado o roubo de identidade. (Aslan & Samet, 2020)

1.2 Phishing

Uma das ramificações do malware, foca-se em utilizar técnicas para convencer os utilizadores a entregar informações sensíveis para serem utilizadas para a concretização de roubos. (Ramzan, 2010)

1.3 Ransomwares

Geralmente utilizado para fazer a cobrança de resgates, este tipo de software de bloqueio ou criptográfico extorque os utilizadores ao incapacitar o dispositivo

eletrônico ao bloqueá-lo ou ao encriptar todos os documentos que estão inseridos nesse dispositivo. (O’Gorman & McDonald, 2012)

2 PANORAMA DA SOCIEDADE

2.1 Implementação de políticas

É possível aplicar uma série de medidas e leis para a prevenção e gestão de riscos relacionados à segurança de sistemas de rede de informação e de entidades, as medidas podem ser adotadas quer a nível organizacional (por ex. regulamento de empresa), a nível nacional (por ex. aprovação de propostas de lei relacionada à cibersegurança) e a nível europeu (por ex. tomada de decisões por parte do parlamento europeu da UE). Além disso existe diversos tipos de leis e de medidas como por ex. a identificação de ativos críticos, a utilização de princípios de análise de riscos, o uso de sistemas de segurança de informação por de parte de organizações, adoção de formas de comunicação direta e notificação/alarmes para as autoridades. (Dumit, 2023)

2.2 Formação contínua dos colaboradores

Através de palestras, aulas e instruções é possível educar e conscientizar os utilizadores e sobre esta problemática atual. E a forma de como podem garantir a segurança dos dados e de como navegar na internet de maneira segura. (Dumit, 2023)

2.1 Criptografia

A criptografia é um método que codifica dados e oferece uma maior privacidade ao utilizador, muitas vezes feito de ponto por ponto. Atualmente é utilizado em diversas apps como por exemplo What’s app. (Jerónimo et al., 2020)

2.1 Autenticação de dois fatores

A autenticação de dois fatores serve para verificar a verdadeira identidade do usuário e deste modo, mitigar possíveis burlas a quem recorra à tecnologia, principalmente no que se refere a roubo de identidades e de contas bancárias. (Nama & Muludi, 2018)

3 ESTUDO DE CASO FICTÍCIO: CIBERSEGURANÇA NA INOVATEC E O IMPACTO DE UMA VIOLAÇÃO DE DADOS

A Inovatec, uma empresa fictícia de Braga, dedicada a soluções tecnológicas para pequenas e médias empresas, viveu recentemente um dos seus maiores sustos na área de segurança digital. A empresa, com 150 colaboradores, lida com dados sensíveis dos clientes, incluindo dados pessoais e financeiros. Em agosto de 2023, a Inovatec foi alvo de um ataque de *ransomware* que abalou a segurança de toda a organização. Esta experiência foi um alerta essencial para a importância da cibersegurança no dia-a-dia e trouxe várias lições para a equipa.

3.1 O Que Correu Mal?

O problema começou com um email aparentemente inofensivo, mas que trazia um link malicioso. Um dos colaboradores da contabilidade acabou por clicar no link, e o sistema foi infetado. Em

poucos minutos, alguns dos servidores mais críticos da Inovatec foram encriptados, impedindo o acesso a dados essenciais. Durante três dias, a empresa ficou quase paralisada: os sistemas estavam bloqueados, os clientes sem resposta e a confiança na segurança da Inovatec foi abalada. Este foi o ponto de viragem em que a equipa percebeu que a cibersegurança tinha de ser levada mais a sério.

3.2 O Que Estava a Faltar?

Após uma análise ao que correu mal, identificaram três falhas principais que facilitaram o ataque:

Falta de Formação em Cibersegurança – *A maioria dos colaboradores nunca tinha recebido formação prática para lidar com phishing e outras armadilhas digitais.*

Sistemas Desatualizados – *Alguns dos programas usados estavam desatualizados, deixando “portas abertas” para hackers.*

Acesso com Segurança Limitada – *Os colaboradores acediam aos sistemas com uma única senha, sem uma segunda camada de autenticação.*

3.3 Lições que Ficaram

Este ataque foi um alerta importante para a equipa, que retirou algumas lições valiosas:

Formação é Essencial – Sem conhecimento adequado, qualquer pessoa pode, sem querer, abrir as portas para um ataque. Agora sabem que cada colaborador precisa de saber identificar e evitar estas ameaças. *(Dumit, 2023)*

Manter os Sistemas Atualizados é Crucial – A atualização de sistemas e softwares pode prevenir vulnerabilidades e minimizar os riscos. *(Jerónimo et al., 2020)*

Adicionar Camadas de Segurança – Medidas como a autenticação multi-fator podem aumentar a proteção, criando uma barreira extra contra acessos indesejados. *(Nama & Muludi, 2018)*

3.4 Possíveis medidas Adotadas para Melhorar a Segurança

Formação Regular em Cibersegurança – A partir de agora, todos os colaboradores passam por formações de cibersegurança a cada três meses. Estas sessões incluem simulações de phishing, para que saibam responder de forma rápida e eficaz a ameaças reais. *(Gonçalves, 2019)*

Política de Senhas e Autenticação Melhorada – Implementaram a autenticação multi-fator e melhoraram as políticas de senhas, dificultando o acesso não autorizado. *(Nama e Muludi, 2018)*

Monitorização Contínua – Para evitar novos incidentes, a Inovatec estabeleceu uma parceria com uma empresa de cibersegurança para auditorias e monitorização constante de ameaças. *(Aslan e Samet, 2020)*

4 CONCLUSÕES

Este incidente demonstrou à Inovatec que a cibersegurança deve ser uma prioridade constante. Proteger os dados dos clientes e as operações internas exige compromisso diário, principalmente num ambiente digital cada vez mais desafiante.

Desta forma, a experiência reforçou que a segurança da informação deve ser encarada como um processo contínuo. Afinal, tal como a tecnologia avança, também as ameaças evoluem e exigem respostas cada vez mais ágeis e seguras.

REFERENCIAS

- Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. *IEEE access*, 8, 6249-6271.
- Dumit, P. L. (2023). *A realidade da cibersegurança nas organizações portuguesas* (Master's thesis).
- Enes, G., Monteiro, A. B., & Oliveira, F. A Reforma da Cibersegurança na União Europeia. O Regime Jurídico de Cibersegurança Instituído pela Diretiva (UE). *Western Journal of Communication*, 63(3), 382-412.
- Gonçalves, P. F. T. (2022). *Os Novos Desafios à Cibersegurança na União Europeia em Tempos de Pandemia Covid19: De que Forma a Pandemia Covid19 Veio Alterar a Cibersegurança na União Europeia, No Período Compreendido Entre março 2020-março 2021?* (Master's thesis, Universidade da Beira Interior (Portugal)).
- Gonçalves, R. S. (2019). *O fator humano da cibersegurança nas organizações* (Master's thesis, Universidade de Lisboa (Portugal)).
- Hermenegildo, G. F. (2020). *Cibersegurança Na União Europeia e Os Desafios Para a sua Eficácia Perspetivas, Panorama Estratégico e Instrumentos Jurídicos* (Master's thesis, Universidade do Porto (Portugal))
- Jerónimo, P., Andrade, F. C. P., Fonseca, I. C. M., Silva, J. M. M. D. A., Abreu, J. R. S. C., Venâncio, P. D., & Freitas, P. M. (2020). Relatório cibersegurança em Portugal: Ética & Direito.
- Machado, P. (2015). O papel da GNR no contexto da Cibersegurança Nacional.
- Nama, G. F., & Muludi, K. (2018). Implementation of two-factor authentication (2FA) to enhance the security of academic information system. *Journal of Engineering and Applied Sciences*, 13(8), 2209-2220.
- O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Arizona, AZ, USA: Symantec Corporation.
- Ramzan, Z. (2010). Phishing attacks and countermeasures. *Handbook of information and communication security*, 433-448.
- Serrano, I. I. B. (2022). *Cibersegurança na União Europeia: a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos* (Master's thesis, Universidade de Évora).
- SILVEIRA, M., & DOS SANTOS, C. E. (2024). CRIMES CIBERNÉTICOS: UM PANORAMA GERAL SOBRE AS PRINCIPAIS AMEAÇAS. *Revista Científica e-Locução*, 1(25), 25-25.
- Vidal, A. M. (2021). *Políticas de Cibersegurança da União Europeia o Processo de Securitização no Domínio do Ciberespaço* (Master's thesis, Universidade de Aveiro (Portugal)).