REVISTA LATINO-AMERICANA DE ESTUDOS CIENTÍFICOS

V. 03, N.16 Jul./Ago. 2022

A SEGURANÇA DIGITAL NAS PEQUENAS E MÉDIAS EMPRESAS: DESAFIOS E POSSÍVEIS SOLUÇÕES

DIGITAL SECURITY IN SMALL AND MEDIUM-SIZED COMPANIES: CHALLENGES AND POSSIBLE SOLUTIONS

SEGURIDAD DIGITAL EN PEQUEÑAS Y MEDIANAS EMPRESAS: RETOS Y POSIBLES SOLUCIONES

Fábio do Vale
Faculdade INSTED
ORCID – https://orcid.org/0000-0001-8713-309X

Natália Barbosa Belchior
Faculdade INSTED
ORCID – https://orcid.org/0000-0003-3273-2743

Weverton Gomes do Nascimento
Faculdade INSTED
ORCID – https://orcid.org/0000-0002-1067-6392

Marcel Ferreira Yassumoto
Faculdade INSTED
ORCID – https://orcid.org/ 0000-0003-2184-7828

Resumo: O presente artigo aborda sob a ótica dos alunos Análise e Desenvolvimento de Sistemas, da Faculdade Insted, Campo Grande, Mato Grosso do Sul, a informatização das pequenas e médias empresas (PMEs) no Brasil que, além de trazer inúmeros benefícios, despertou o interesse de cibercriminosos que têm se aproveitado de seus frágeis, e até mesmo inexistentes, sistemas de segurança digital. Neste artigo explanaremos sobre quais as principais formas de atuação dos hackers e quais os seus interesses em atacar as PMEs, pois ao entender seu modus operandi é possível propor meios de evitá-los e combate-los. Diante disso, reforçamos a necessidade de falar sobre a importância da segurança digital nas PMEs, para que tomem conhecimento e entendam os riscos que correm por não agirem de forma preventiva.

Palavras-chave: Segurança digital. PMEs. Ciberataques. Cibersegurança.

Abstract: This article discusses, from the point of view of Systems Analysis and Development students, from Faculdade Insted, Campo Grande, Mato Grosso do Sul, the computerization of small and medium-sized companies (SMEs) in Brazil, which, in addition to bringing numerous benefits, aroused the interest of cybercriminals who

have taken advantage of its fragile, even non-existent, digital security systems. In this article, we will explain the main ways in which hackers act and what their interests are in attacking SMEs, because by understanding their modus operandi it is possible to propose ways to avoid and combat them. In view of this, we reinforce the need to talk about the importance of digital security in SMEs, so that they become aware and understand the risks they run for not acting in a preventive way.

Keywords: Digital security. PMEs. cyberattacks. Cybersecurity.

Resumen: Este artículo discute, desde el punto de vista de estudiantes de Análisis y Desarrollo de Sistemas, de la Faculdade Insted, Campo Grande, Mato Grosso do Sul, la informatización de las pequeñas y medianas empresas (PYME) en Brasil, que además de traer numerosos beneficios, despertó el interés de los ciberdelincuentes que se han aprovechado de sus frágiles, incluso inexistentes, sistemas de seguridad digital. En este artículo explicaremos las principales formas en que actúan los hackers y cuáles son sus intereses al atacar a las pymes, pues al comprender su modus operandi es posible proponer formas de evitarlos y combatirlos. Ante esto, reforzamos la necesidad de hablar sobre la importancia de la seguridad digital en las PYMES, para que tomen conciencia y comprendan los riesgos que corren por no actuar de manera preventiva.

Palabras-clave: Seguridad digital. PMEs. Ataques ciberneticos. La seguridad cibernética.

Introdução

> Eu sou apenas um rapaz latino-americano. Sem dinheiro no banco, sem parentes importantes. E vindo do interior (BELCHIOR, 1976.).

A era digital trouxe para a sociedade brasileira as mais diversas melhorias, incluindo a forma de consumir e trabalhar das pessoas. E, buscando se tornar mais competitivas e atrativas, as pequenas e médias empresas (PMEs) também transformaram a sua forma de trabalho e de interação com os clientes, no entanto junto com toda a agilidade e alcance propiciado pela conectividade, vieram os ataques cibernéticos.

No cenário brasileiro, as PMEs demonstram sua força perante a economia, representando em torno de 30% do produto interno bruto (PIB), porém quando o assunto é segurança digital ainda são extremamente frágeis. O desconhecimento quanto aos principais tipos de golpes e crimes cometidos somados a falta de investimento em cibersegurança os leva a ser

alvo de grande interesse dos hackers, os resultados desses ataques podem ser tão nocivos as empresas levando-as ao ponto de encerrarem suas atividades.

O interesse por parte dos criminosos com relação as empresas brasileiras se refletem no fato do país ser líder em alguns tipos de golpe. Para isso os mesmos se utilizam da boa-fé e desconhecimento do usuário (seja ele funcionário ou empresário) e das vulnerabilidades que, na maioria das vezes, é criada pelo próprio usuário. Com o intuito de despertar a sociedade brasileira para a importância da segurança digital, falaremos sobre essas fragilidades e as possíveis formas de atenuá-las.

Desenvolvimento

> A primeira regra de qualquer tecnologia utilizada nos negócios é que a automação aplicada a uma operação eficiente aumentará a eficiência. A segunda é que a automação aplicada a uma operação ineficiente aumentará a ineficiência. (BILL GATES).

Frequentemente invasores atacam e comprometem de forma ativa o desempenho e a segurança das pequenas e médias empresas (PMEs), o cenário que vemos hoje na cibersegurança está se tornando mais preocupante pois, na grande maioria das vezes, as empresas não contam com sistemas de segurança e só percebem a necessidade do investimento após algum ataque hacker, algo que poderia ser evitado se fosse dado a devida importância para a Segurança da Informação. De acordo com as principais pesquisas de mercado, mais de 50% de todos os ataques cibernéticos dos últimos anos foram endereçados aos PCs e usuários das PMEs.

Um dos motivos para o não investimento na área é a questão financeira, diferentemente das empresas de grande porte que conseguem fazer altos investimentos em segurança da informação, as PMEs possuem orçamentos enxutos e por isso acabam voltando a maior parte dos investimentos para o aumento de produtividade, e em muitos casos as

mesmas acabam fazendo uso de programas piratas e cracks, conforme exposto no relatório divulgado pela Kaspersky, intitulado "Como as pequenas empresas superaram as dificuldades de 2020-2021: cortes de orçamento, lançamentos de produtos e novas prioridades de investimento", esse tipo de programa quebra a proteção do software original, contribuindo com a exposição da empresa.

Outro motivo é a falsa sensação de que o ambiente virtual é seguro e que não são um alvo para os criminosos, isso faz com que empresários não busquem conhecer seus riscos e, consequentemente, não façam investimentos na área de segurança virtual. Além disso, muitas vezes tanto empresários, quanto colaboradores acabam utilizando seus dispositivos (seja mobile ou desktop) e redes pessoais para fins profissionais. E de acordo com Michael Dortch, no texto "Ataques cibernéticos: os desafios para pequenas empresas" (2019), "Isso significa que todas as ameaças que desafiam os consumidores, desafiam igualmente as pequenas empresas."

Segundo o relatório "Panorama de Ameaças 2021" divulgado pela empresa de cibersegurança Kaspersky, o Brasil é líder em tentativas de infecção por malware na América Latina, são 1395 tentativas por minuto. Os malwares (malicious software) em português software malicioso, são programas projetados com o intuito de explorar, sequestrar e danificar, alguns exemplos de malwares mais conhecidos são os vírus e cavalo de Tróia. Os softwares maliciosos têm potencial de infectar computadores, dispositivos, serviços e redes programáveis, causando variados problemas pois cada software age de acordo com o seu objetivo. Sua propagação ocorre ao clicar em links ou baixar anexo de e-mails (phishing), instalação de aplicativos e softwares gratuitos infectados, conectar unidades USB infectadas, mensagens de texto via celular e anúncios publicitários maliciosos (phishing).

Apesar dos malwares serem desenvolvidos de forma a evitar serem detectado por antivírus, há algumas formas de se identificar uma possível infecção, como: a perda de desempenho, o dispositivo fica lento; anúncios

pop-up incessantes; redirecionamento do navegador para sites aleatórios; interrupção de funcionamento do dispositivo inesperadamente; e travamento da máquina.

A fim de evitar os malwares é necessário que os usuários seja vigilantes com os links e sites que abrem, onde clicam e com o que estão baixando; manter em dia as atualizações de sistemas e outros softwares, pois os hackers procuram brechas em programas desatualizados; e utilizar programa de proteção contra malware, o antivírus, e fazer varreduras constantes.

O país também é líder em ataques de phishing e ransomware. No phishing, os hackers se passam por grandes companhias dos mais diversos setores, incluindo os bancos, fazendo com que as vítimas acreditem na veracidade da informação que está sendo passada, para isso os criminosos se utilizam, principalmente, de e-mails, SMS e mensagens instantâneas, que contém uma mensagem que induz os usuários a clicar em links, que parecem estar em um endereço, mas o leva para outro, ou baixar anexos, que possuem malwares. A intenção é sempre fazer com que as pessoas forneçam dados pessoais ou empresariais, senhas, logins e acesso aos dispositivos de forma voluntária, consequentemente levando a perdas financeiras como retiradas de valores de contas bancárias e uso de cartões de crédito e roubo de identidade o que leva a aplicação de novos golpes.

Algumas maneiras de se evitar o phishing é utilizando softwares de antivírus, mantendo-o atualizado, e fazer treinamento dos funcionários para que saibam reconhecer se o link pode ser falso e não forneça dados sem se certificar de que é seguro, enfim consigam reconhecer quando recebem uma mensagem mal intencionada. Contar com o bom senso do funcionário é imprescindível, pois eles são a porta de acesso da empresa para os cibercriminosos.

O ransomware é um tipo de software malicioso, que tem como objetivo sequestrar um dispositivo, seja ele um computador ou rede de computadores, smartphone, servidor, entre outros. Após a infecção, o

malware irá criptografar os dados e bloqueará o acesso ao sistema, posteriormente emitirá um aviso informando o ataque e solicitará um resgate (ransom), que deverá ser pago em criptomoeda, para liberar o acesso, caso contrário tudo será perdido.

O prejuízo causado pelo ransomware vai além do resgate, caso a empresa opte por pagá-lo (e não há garantia de que os criminosos irão cumprir o acordo), há o prejuízo da paralisação das operações que podem durar dias ou semanas, perda de clientes por falta de confiança e custo para restabelecer o sistema.

Uma forma de mitigar as consequências desse tipo de ataque é fazer backups periodicamente, seja em dispositivos externos de armazenamento físico ou nuvem. Por se tratar de um tipo de malware, sua infecção ocorre da mesma forma que os outros tipos de software maliciosos e também se faz necessário uso de antivírus, juntamente com ferramentas anti-ransomware (são ferramentas que, em sua maioria, conseguem detectar e bloquear o software).

Os vazamentos de dados empresariais têm como uma de suas principais consequências o acesso indevido de criminosos a informações confidenciais. Quando dados financeiros e/ou credenciais de acesso (como informações de e-mail e senha) chegam às mãos de pessoas mal-intencionadas, podem ser usados para as mais diversas finalidades ilícitas. Independentemente do modo como sua empresa é vitimada, pode haver consequências a curto e a longo prazo para todos os envolvidos.

> Dados recentes levantados pela PSafe, unidade de cibersegurança do Grupo CyberLabs, expõe que os vazamentos de dados em 2021 ultrapassaram os 4.6 bilhões de credenciais vazadas no mundo. Este tipo de ameaça tem desafiado a segurança, especialmente das pequenas e médias empresas, que têm visto seus colaboradores como maiores alvos dos ataques. Uma pesquisa realizada pela PSafe mostram que: 75% das empresas que checaram se tiveram dados vazados, usando a ferramenta gratuita "Verificador de Vazamentos" do site do dfndr enterprise, de fato descobriram que tinham dados expostos na Internet. O alto número

> evidencia que uma grande parte das empresas brasileiras ainda possui métodos de proteção frágeis contra os vazamentos de dados, o que os torna alvos extremamente atrativos para cibercriminosos (THAISY PECSEN, 2021, As 6 consequências mais devastadoras de um vazamento de dados corporativos).

Hoje, dados importantes estão arquivados em ambientes virtuais como as nuvens e qualquer violação em sistemas causa grande prejuízo para as empresas. Empresas pequenas são justamente as que correm os maiores riscos por serem alvos mais atrativos para os hackers.

É importante enfatizar, a responsabilidade que a empresa tem em relação aos dados de seus clientes e segurança das informações confidenciais da empresa. Sendo que existem empresas especializadas em segurança digital, garantindo a ciberseguarança e prestando serviços de suporte e softwares autênticos e devidamente atualizados. Sendo viável para empresa é importante a implantação do setor de T.I, algo recomendado, devido o crescimento de crimes cibernéticos.

Conclusão

> Só por que alguma coisa não faz o que você planejou que ela fizesse não quer dizer que ela seja inútil (Thomas Edison).

Os crimes ciberneticos evoluem na mesma velocidade em que as tecnologias são desenvolvidas, logo, não deixarão de existir. Portanto, as empresas e seus usuários também devem se atualizar continuamente, isso não significa que as empresas nunca serão vítimas, mas isso reduzirá consideravelmente as chances de possíveis infecções. Os criminosos procuram por vulnerabilidades para atacar, enquanto a segurança digital buscar extinguir qualquer brecha que possa trazer danos.

Para aprimorar a segurança de seus ambientes e maximizar resultados, as PMEs devem mudar sua postura. O primeiro passo é entender a cibersegurança como parte central da estratégia de negócios. Os empresários precisam assimilar a importância do tema, adotar uma

mentalidade voltada à segurança e, além disso, considerar que todos os elementos são importantes para garantir a proteção de seus dados – começando por orientações e políticas de acesso envolvendo os funcionários.

Criar uma cultura corporativa orientada à segurança deve incluir os usuários nas discussões sobre o assunto, capacitando-os para agir de maneira segura e proativa, além de permitir que as companhias ampliem suas camadas de proteção para prevenir e combater as possíveis vulnerabilidades da operação. É importante desenvolver uma cultura de cibersegurança que envolva toda a organização. As PMEs devem aprimorar suas infraestruturas, reforçando as ferramentas de segurança à disposição dos negócios. Com a tecnologia evoluindo rapidamente, é imprescindível implementar soluções modernas, preparadas para garantir com eficiência a integridade de seus dados.

Referências

Aprenda sobre malware e como proteger todos os seus dispositivos contra eles. 2021. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it. Acesso: 20 nov. 2021.

O desafio da segurança digital em pequenas e médias empresas. 2019. Disponível em: https://www.consumidormoderno.com.br/2019/03/07/desafio-seguranca-digital-pequenas-medias-empresas. Acesso: 21 nov. 2021.

BELBIC, Ivan. **O que é Malware?.** 2019 . Disponível em: https://www.avast.com/pt-br/c-malware#gref. Acesso: 20 nov. 2021.

BELBIC, Ivan. **O guia essencial sobre phishing: Como funciona e como se proteger.** 2020. Disponível em: https://www.avast.com/pt-br/c-phishing#gref. Acesso: 19 nov. 2021.

DORTCH, Michael. **Ataques cibernéticos: os desafios para pequenas empresas.** Huawai Cloud, 2020. Disponível em: https://huaweibra.com.br/blog/seguranca/ataques-ciberneticos/. Acesso em: 19 nov. 2021.

Dicas para a prevenção de phishing. 2021. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips. Acesso: 19 nov. 2021.

DE SOUZA, Ivan. **Saiba o que é segurança digital e como implantá-la no site da sua empresa.** 2020. Disponível em: https://rockcontent.com/br/blog/seguranca-digital/. Acesso: 20 nov. 2021.

JAJONE, Lucas. **Ataques cibernéticos a empresas brasileiras crescem 220% no 1º semestre de 2021.** 2021. Disponível em: https://www.cnnbrasil.com.br/business/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021/. Acesso: 21 nov. 2021.

O que é malware. McAfee, 2021. Disponível em: https://www.mcafee.com/pt-br/antivirus/malware.html. Acesso em: 20 nov. 2021.

O que é phishing e por que você precisa fugir disso? 2020. Disponível em: https://www.meuportoseguro.com.br/minha-vida/tecnologia/o-que-e-phishing-e-por-que-voce-precisa-fugir-disso/. Acesso: 19 nov. 2021

Reconhecendo um ransomware – diferenças entre cavalos de troia de criptografia. 2021. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-attacks-and-types. Acesso: 20 nov. 2021.

Segurança digital para pmes: como se prevenir e preparar para ataques? 2021. Disponível em: https://vivomeunegocio.com.br/conteudos-gerais/gerenciar/seguranca-digital-para-pme/. Acesso: 19 nov. 2021.

Startups e pmes estão na mira dos ataques de ransomware. 2020. Disponível em: https://www.unxpose.com/post/startups-e-pmes-est%C3%A3o-na-mira-dos-ataques-de-ransomware. Acesso: 20 nov. 2021.

Revista Latino-Americana de Estudos Cientifico - RELAEC
Disponível em: https://periodicos.ufes.br/ipa/index
ISSN: 2675-3855