Monumenta - Revista Científica Multidisciplinar

Artigos

A Relevância da segurança de redes em empresas contábeis e estratégias para fortalecer a infraestrutura de rede

The relevance of network security in accounting firms and strategies to strengthen network infrastructure

Pedro Henrique Ewen[1]
Emanoel Guilherme Barros[2]

[1]União Educacional Cultural e Tecnológica Vincit Ltda.
[2]Centro Universitário Maurício de Nassau.

✉ pedrohenriquewen@gmail.com
✉ e.guilhermebarros@outlook.com

Palavras-chave:
Segurança Cibernética;
Lei Geral de Proteção de Dados;
Empresas.

Resumo

Na sociedade atual, observa-se uma crescente onda de ataques cibernéticos e o modelo de serviço *ransomware-as-a-service* (RaaS), no qual códigos são vendidos por gangues especializadas a outros hackers para atacar empresas, Assim, é imperativo que as empresas implantem políticas de segurança e conscientizem seus funcionários sobre boas práticas de segurança cibernética, visto que um dos vetores de ataque mais eficientes é o ser humano. O presente artigo objetivou identificar como as empresas de contabilidade desempenham a segurança cibernética, bem como mostrar para as empresas sobre a importância da segurança cibernética e citar ferramentas para melhorá-la. Para a realização da pesquisa, foi realizado o contato telefônico com empresas de contabilidade localizadas em Recife-PE, no período de julho de 2023. Com as devidas permissões, efetuado as perguntas que originaram os dados expostos neste artigo. Os resultados da pesquisa evidenciaram que a maioria das empresas realiza a terceirização dos setores de TI. Em comparação com o que será mostrado, é a decisão mais sensata a ser tomada, uma vez que as empresas de contabilidade trabalham com dados sensíveis de outras empresas e clientes. As ferramentas citadas neste artigo são projetos abertos, onde qualquer indivíduo pode consumi-los sem qualquer custo ou licença. Como o PFsense, Zabbix, Veeam, Wazuh, Snort e OpenVAS. Bem como a realização de testes de intrusão para certificar e atestar a segurança da rede corporativa. Conclui-se que, inicialmente, não é necessário um grande gasto com ferramentas de primeira linha para garantir a segurança das informações e da infraestrutura de rede.

Keywords:
Cybersecurity;
General Data Protection Regulation;
Companies.

Abtract

In today's society, we observe a growing wave of cyber attacks and the ransomware-as-a-service (RaaS) model, in which codes are sold by specialized gangs to other hackers to target companies. Therefore, it is imperative for companies to implement security policies and raise awareness among their employees about good cybersecurity practices, as one of the most efficient attack vectors is the human element. This article aimed to identify how accounting firms perform cybersecurity, as well as to emphasize to companies the importance of cybersecurity and mention tools to enhance it. To conduct the research, phone contact was made with accounting firms located in Recife, Brazil, during July 2023. With the necessary permissions, questions were asked that led to the data presented in this article. The research results showed that the majority

of firms outsource their IT departments. In comparison to what will be shown, it is the most sensible decision to be made, since accounting firms deal with sensitive data from other companies and clients. The tools mentioned in this article are open-source projects, where any individual can use them at no cost or license, such as PFsense, Zabbix, Veeam, Wazuh, Snort, and OpenVAS. Additionally, conducting intrusion tests to ensure and certify the security of the corporate network is recommended. It is concluded that initially, there is no need for a significant investment in top-tier tools to ensure the security of information and network infrastructure.

1 INTRODUÇÃO

Desde a aprovação da Lei Geral de Proteção de Dados (LGPD), muitas empresas foram obrigadas a dar a devida importância aos dados pessoais dos seus clientes e adequar-se com os parâmetros impostos pela lei. Porém, no cenário encontrado no mercado atual, as empresas não investem em proteção para suas redes corporativas ou capacitam seus funcionários para que possam coletar, tratar e armazenar de forma correta os dados pessoais dos seus clientes. O custo para ter uma rede corporativa "segura" é alto, e existem no mercado milhares de marcas com dispositivos de segurança diferentes dispostos a venderem cada vez mais funções embarcadas em seus produtos para dispor as empresas de um falso senso de segurança em um único produto.

A pesquisa foi realizada visando as empresas de contabilidade por trabalharem com dados sensíveis de outras empresas, tendo em mente que existem organizações que não possuem setor administrativo e buscam a terceirização do mesmo para a redução de gastos. Porém, não somente empresas são afetadas como também microempreendedores individuais (MEI), Pessoas jurídicas (PJ) e clientes que recorrem de seus serviços de contabilidade.

Desse modo, por que as empresas de contabilidade não realizam investimento em ferramentas e profissionais qualificados para manter a segurança das informações dos seus clientes? Torna-se cada vez mais distante a realidade em que as empresas investem na segurança cibernética dos dados dos seus clientes. Frisando que não há segurança absoluta, esse artigo aborda sobre a importância da segurança cibernética e dos dispositivos que a proporcionam.

2 OBJETIVO

A presente pesquisa teve como objetivo identificar como as empresas de contabilidade desempenham a segurança cibernética, bem como mostrar para as empresas sobre a importância da segurança cibernética, a custo baixo e citar ferramentas para melhorá-la.

3 MÉTODOS

Foi desenvolvida uma pesquisa quantitativa, na qual visou catalogar informações relevantes para o artigo. No período de coleta de informações, foi realizado o contato telefônico com empresas de contabilidade localizadas em Recife-PE, no período de julho de 2023. Com as devidas permissões, efetuado as perguntas que originaram os dados expostos neste artigo.

4 RESULTADOS E DISCUSSÕES

A amostra da pesquisa consiste em 59 empresas de contabilidade de Recife, contatadas via ligações telefônicas, explicando sobre o motivo da pesquisa. Desse modo, foi questionado se a empresa possuía setor de tecnologia da informação (TI), e caso tivesse, se a empresa adotava o uso do Firewall.

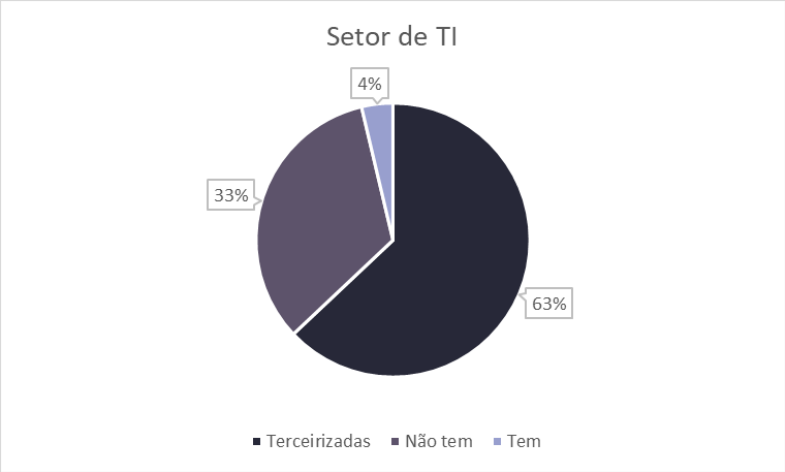
Inicialmente o contato foi realizado com uma pessoa não técnica e que não soube responder às questões. Então foi adotada uma metodologia diferente, começando por entender como se dá a infraestrutura de tecnologia da informação da empresa e assim, sendo direcionado para o funcionário responsável ou empresa terceirizada.

Com base na pesquisa, a maioria das empresas realiza a terceirização dos setores de TI. Em comparação com o que será mostrado, é a decisão mais sensata a ser tomada, uma vez que as empresas de contabilidade trabalham com dados sensíveis de outras empresas e clientes. Consequentemente, a terceirizada é responsável por toda questão de segurança de rede, correção de vulnerabilidades, monitoramento de ativos e aplicação de patchs de segurança, diminuindo a preocupação da contratante sobre determinadas questões.

Em contrapartida, temos as empresas que não se importam com a segurança cibernética e expuseram-se a potenciais ameaças. Com o avanço da tecnologia, a criação de cada vez mais vetores de ataque estão surgindo e cabe às organizações investirem em um setor de TI, profissionais, e dispositivos que proporcionam a proteção apropriada para a rede corporativa.

O Gráfico 1 mostra como é a segmentação de empresas quanto a presença de um setor responsável pela tecnologia da informação.

Gráfico 1 - Setor de TI



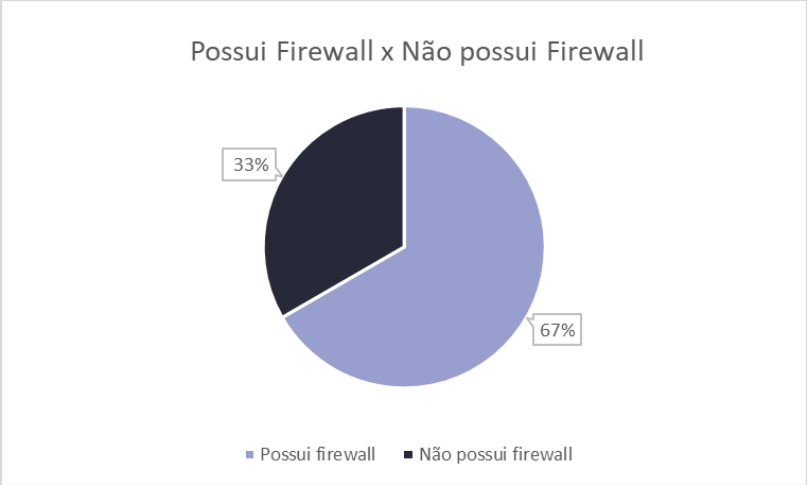
Fonte: Elaborado pelo autor.

Analisando o Gráfico 1, é possível observar que 33% das empresas de contabilidade não investem na proteção de dados e na segurança de rede. Até mesmo não optaram pela solução mais simples, como 63% das organizações que terceirizam o setor. Outra solução que poderia ser tomada seria a contratação de um consultor que realizaria as demandas do âmbito de tecnologia, fortalecendo a infraestrutura de rede do negócio.

A LGPD (Lei nº 13.709/18) institui que as entidades sejam responsáveis pelo armazenamento seguro das informações, e em caso de violação da mesma, a organização pode sofrer diversas sanções que podem acarretar multas e até a proibição das atividades relacionadas às informações. Segundo o Art. 52, II e III, da Lei nº 13.709/18, as sanções incluem multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração e multa diária, observado o limite total a que se refere o inciso II (Brasil, 2018, Capítulo VIII).

Como referido acima as sanções administrativas podem causar o colapso da organização e publicização das infrações, o que fere a imagem moral e provoca a perda de clientes, fornecedores e parceiros.
Outra perspectiva é a das empresas que possuem dispositivos como firewall (Gráfico 2) que auxiliam na preservação da proteção dos dados dos seus clientes. No entanto, somente um dispositivo não é o suficiente para desempenhar a defesa da rede, é aqui que entram alguns softwares e equipamentos comumente usados para ampliação da proteção e o monitoramento dos ativos de rede.

Gráfico 2 - Possui ou não possui Firewall



Fonte: Elaborado pelo autor.

Muitas das ferramentas que serão citadas neste artigo são projetos abertos, onde qualquer indivíduo pode consumi-los sem qualquer custo ou licença. É claro que alguns vendem o suporte como serviço, mas não será pontuado.

O PFsense é um firewall e roteador open-source que atua nas camadas de rede e transporte, realizando a filtragem de pacotes. Entre outras funções como a elaboração de filtro de conteúdo, regras de acesso, criação de redes virtuais privadas (VPN´S), servidor de Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Network Address Translation (NAT), balanceamento de carga e Failover. O PFsense pode ser virtualizado para a redução de gastos com appliance.

O Zabbix é uma ferramenta de monitoramento de rede completa e também complexa, é possível monitorar qualquer tipo de ativos de rede, como roteadores, firewall, servidores, conexões, banco de dados. Além disso, é possível realizar automações dependendo do acionamento que for criado pelo administrador. Também é capaz de enviar notificações por meio de integrações de softwares compatíveis. Uma ótima integração é com o Grafana, que é uma ferramenta para visualização e desenvolvimento de dashboards, permitindo criar melhores gráficos e dashboard para monitoramento mais eficiente e amigável, levando em consideração que os gráficos do Zabbix são limitados em relação à customização. Sendo ambas ferramentas virtualizadas, como mencionado acima, reduz ainda mais os custos.

O Veeam é um software de backup open-source que permite realizar cópias e restauração de dados em diferentes sistemas operacionais, a ferramenta permite a execução de backup de arquivos, pastas, volumes, banco de dados, entre outros. Permite o agendamento de tarefas, cópia em tempo real, notificações por e-mail, a criação de relatórios detalhados e adição de scripts personalizados. Existem também a integração com a AWS, Azure, Microsoft 365 e Google Cloud. Mais uma ferramenta virtualizada com suporte a diversos dispositivos.

O Wazuh é um Security Information and Event Management (SIEM), uma ferramenta de monitoramento e controle de eventos. Diferentemente do Zabbix, o Wazuh tem foco em monitorar registro e logs de eventos. Com ele é possível analisar e-mails, filtros de tráfego de rede e o comportamento de agentes de rede. Ademais existem os Dashboards para a visualização do administrador. Como é uma ferramenta totalmente virtualizada irá reduzir ainda mais custos da infraestrutura de rede.

O Snort é um Intrusion Prevention System (IPS), um sistema de prevenção de intrusões que realiza a captura e registro de pacotes em tempo real. Usando o Snort, é possível que o administrador identifique uma anomalia na rede, como um Scan de portas com a ferramenta Network Mapper (NMAP), ataques de negação de serviço (DoS) e ataques de serviço distribuídos (DDoS). Pode ser integrado ao PFsense para maior robustez na segurança de rede.

O OpenVAS é um scanner de vulnerabilidades completo que realiza a varredura de rede analisando possíveis falhas e má configurações na segurança de sistemas, redes, hosts e aplicativos. Ele executa a busca com base em seu banco de dados de vulnerabilidades de softwares e protocolos de rede. A ferramenta fornece relatórios detalhados sobre as vulnerabilidades encontradas. Assim, ajudando as empresas a identificarem e corrigirem as falhas antes que possam ser exploradas.

Essas são algumas das milhares de ferramentas open-source que podem ser implantadas para aumentar a proteção de uma rede corporativa, cada ferramenta possui determinadas funções e muitas podem ser integradas melhorar seu funcionamento e a abrangência. No entanto, vale salientar que não é somente os softwares e equipamentos que proporcionam a segurança da rede, precisam realizar a conscientização dos funcionários sobre as políticas de segurança da informação (PSI) e a LGPD.

A realização de testes de intrusão para certificar e atestar a segurança da rede corporativa é de suma importância, com o passar do tempo, mais vulnerabilidades vão surgindo, e os profissionais e empresas precisam manter-se atualizados quanto às ferramentas e softwares que utilizam em sua infraestrutura. Além disso, o investimento no treinamento dos profissionais de segurança da informação também é essencial para acompanhar as evoluções tecnológicas e as ameaças.

Sobre os testes de intrusão, eles podem ser realizados periodicamente a cada 3 meses por um profissional qualificado expondo assim as falhas e vulnerabilidades. Desse modo, o colaborador contratado para atuar na proteção da rede poderá corrigir e estar pronto para o próximo teste. É um círculo vicioso que não pode ser contido, sempre haverá novas vulnerabilidades e sempre serão necessárias corrigi-las.

5 CONSIDERAÇÕES FINAIS

No desenvolvimento da pesquisa foi identificado que a maioria das empresas de contabilidade evidenciadas na amostra, não desempenham adequadamente a segurança cibernética, tampouco tem ideia da importância e da criticidade do tema para as organizações.

Desse modo, nesse artigo foi apresentado algumas das diversas ferramentas gratuitas que podem ser aplicadas em organizações de diferentes tamanhos, e assim, chega-se à conclusão que não existe razão para que as empresas não invistam setores de tecnologia da informação, especialmente considerando a redução de custos com equipamentos essenciais mencionados no artigo.

Porém, as ferramentas automatizadas não podem substituir um bom profissional que está sempre monitorando, efetuando patches de segurança, aprimorando-se, exercendo melhorias na segurança da rede, implantando novas ferramentas e scripts para proteger a infraestrutura.

A presença do profissional de segurança da informação é de suma importância para as empresas. Pois ele desempenha o papel de executor dos testes de intrusão e produz o relatório contendo todas as falhas para a correção de vulnerabilidades da empresa. Além do mais, poderá realizar os treinamentos de conscientização dos colaboradores sobre ameaças cibernéticas, a mitigação de vulnerabilidades e a prevenção de ataques.

REFERÊNCIAS

BRASIL. LEI Nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Diário Oficial da União, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 de abr. de 2024

OPENVAS. **OpenVAS - Open Vulnerability Assessment Scanner**. 2006. Disponível em: https://www.openvas.org/. Acesso em: 30 de abr. 2024

PFSENSE. **pfSense - World 's Most Trusted Open Source Firewall**. 2005. Disponível em: https://www.pfsense.org/. Acesso em: 30 de abr. 2024

SNORT. **Snort - Network Intrusion Detection & Prevention System**. 2000. Disponível em: https://www.snort.org/. Acesso em: 30 de abr. 2024

VEEAM. **Software de backup, recuperação e proteção de dados moderna.** Veeam. 2006. Disponível em: https://www.veeam.com/pt. Acesso em: 30 de abr. 2024

WAZUH. **Wazuh - Open Source XDR.** Open Source SIEM. 2008. Disponível em: https://wazuh.com/ . Acesso em: 30 de abr. 2024

ZABBIX. **Zabbix:** The Enterprise-Class Open Source Networking Monitoring Solution. 2004. Disponível em: https://www.zabbix.com/. Acesso em: 30 de abr. 2024.