POR QUE *CIBERSECURITY* DEVERIA SER PRIORIDADE PARA AS EMPRESAS?

Leidivino Natal

A transformação digital e o rápido avanço tecnológico dos últimos anos fizeram com que o setor de TI (tecnologia da informação) assumisse um papel estratégico nas organizações. Os dados utilizados para as tomadas de decisão se tornaram verdadeiros ativos e, consequentemente, precisaram ser gerenciados com mais eficiência.

O ano de 2020 ficou marcado como um ano atípico. De potencial virada econômica, o ano foi palco de uma crise sanitária e política sem precedentes jamais vista, de alcance global. O mundo do trabalho teve que se reinventar às pressas e transformações que estavam em vias de desenvolvimento paulatino tiveram um *speedup* repentino, que fizeram muitas empresas redesenharem suas estratégias. O digital não é mais uma opção, um *add-on* ou um benefício da rotina. É a realidade de muitas empresas. Com as mudanças, as pessoas em casa sendo os novos *targets* a serem alcançados, os dados ganharam um lugar de protagonismo nas estratégias.

O ritmo da transformação digital não foi acompanhado de proteção suficiente para um novo modelo de trabalho que tornou os dados das organizações mais vulneráveis, com acessos através de mais aparelhos móveis e conexões domésticas. A informação extrapolou o escritório e as organizações precisaram redesenhar suas políticas de segurança com o foco na proteção dos endpoints.

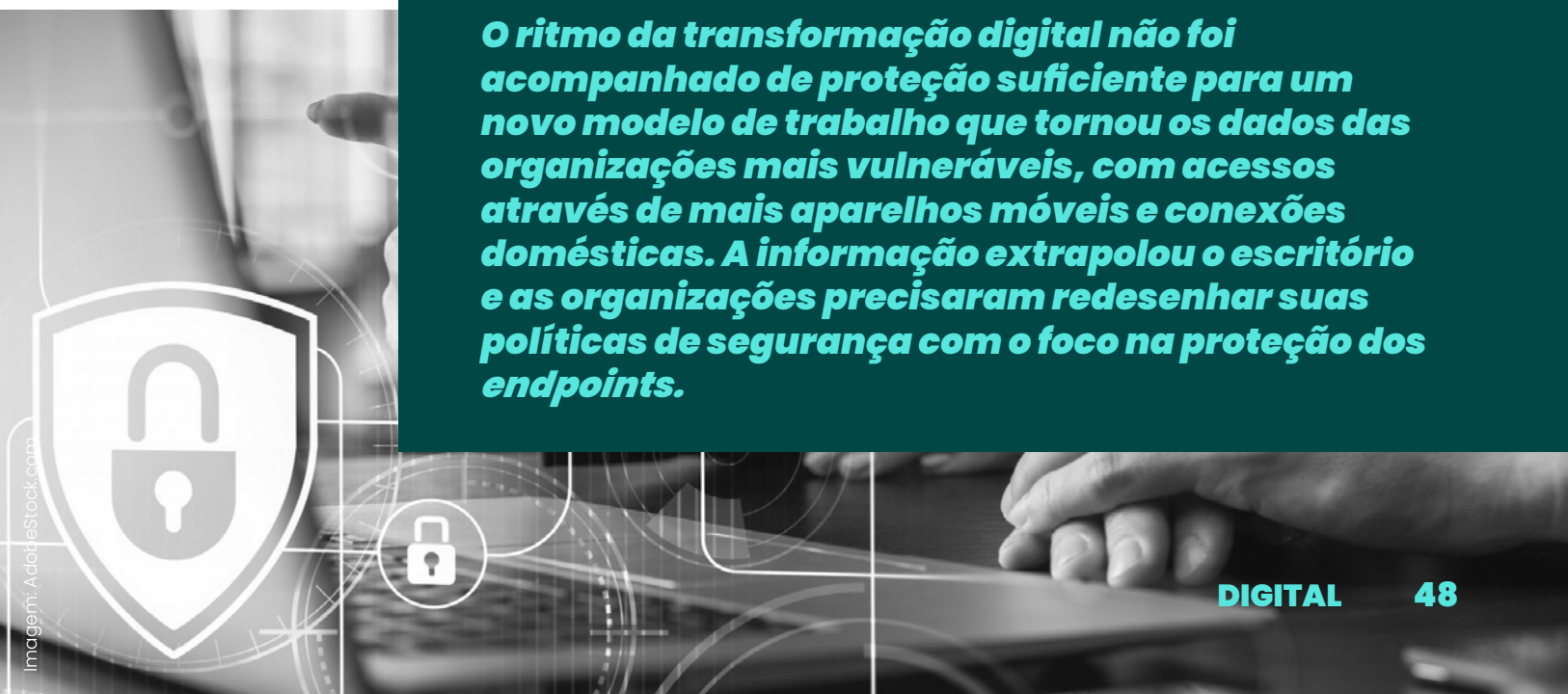
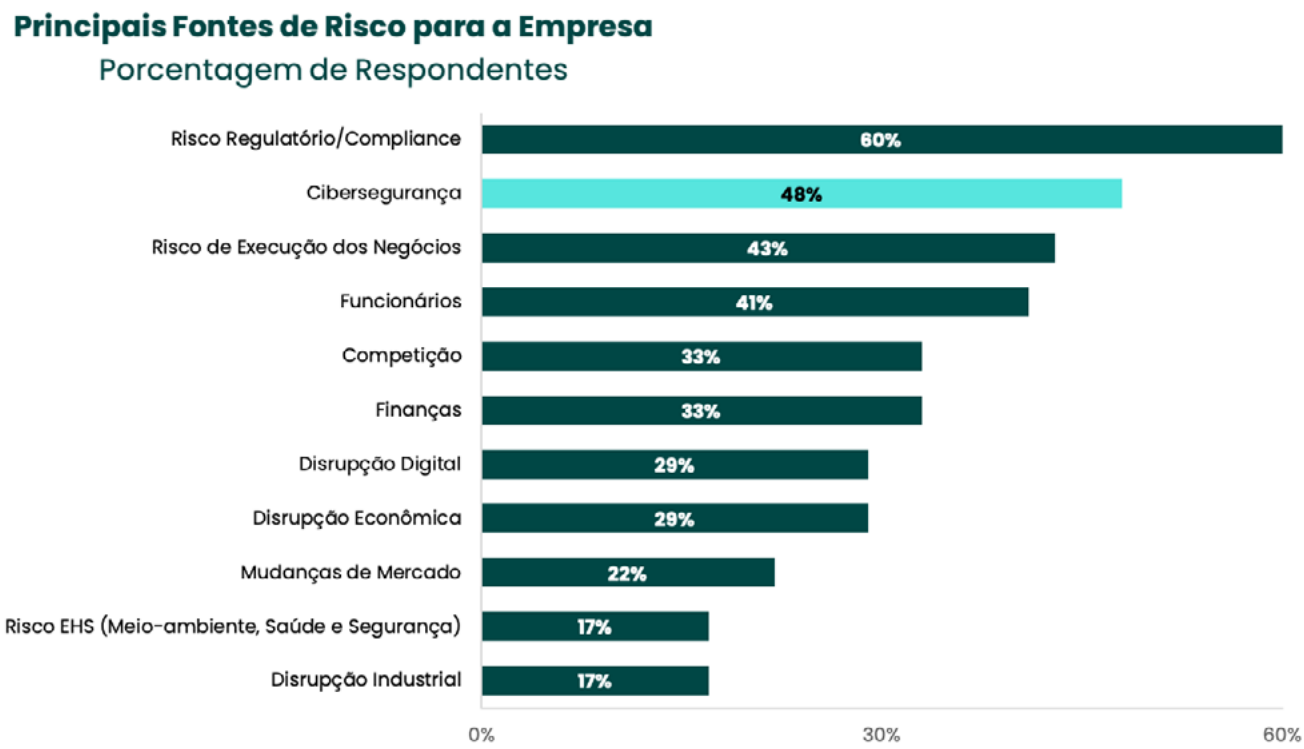


Imagem: AdobeStock.com

Todos nós, quase que semanalmente, lemos notícias sobre um grupo de *hackers* que invadiu sistemas empresariais, bancários ou até mesmo governamentais, causando caos e prejuízos financeiros. Somente no primeiro trimestre deste ano ocorreram 3,2 bilhões de ataques cibernéticos no Brasil, figurando o nosso país como líder no *ranking* de países latinos.[1]

Nesse cenário, a segurança da informação nas empresas ganhou destaque e passou de um item no *checklist* de projetos para a continuidade do negócio e posicionamento das organizações no mercado.

De acordo com pesquisa realizada pelo Gartner (2020), atualmente, a segurança cibernética é a 2ª maior preocupação dos Conselhos Estratégicos das organizações, ficando atrás apenas de compliance[2].



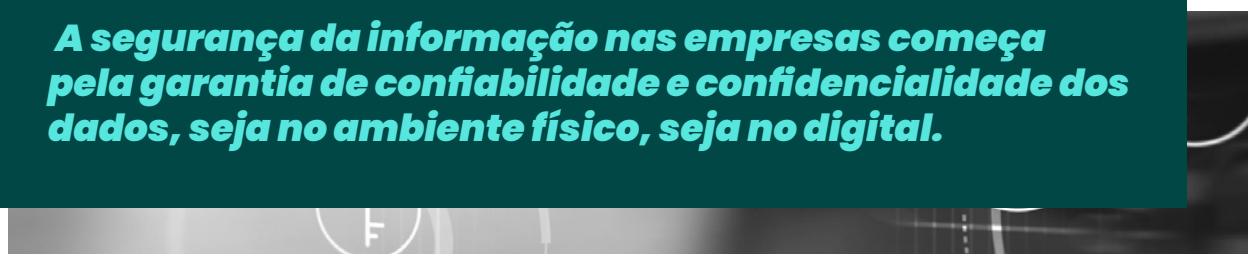
POR QUE A SEGURANÇA DEVE ESTAR NA SUA LISTA DE PRIORIDADES?

AMEAÇA À CONFIDENCIALIDADE DOS DADOS

A confidencialidade é muito mais do que simplesmente manter os dados da empresa protegidos a sete chaves. O conceito, que está entre os pilares da segurança da informação, não se trata de bloquear os dados, mas de se ter governança sobre quem são as pessoas autorizadas a acessá-los. A falta de atenção a este tópico pode acarretar severos prejuízos às organizações, pois além da possibilidade de um sistema sair do ar e prejudicar operações, o vazamento pode significar que pessoas estão acessando informações sensíveis e que sua gestão de segurança está vulnerável.

Se esse tipo de informação é roubado ou vaza de alguma forma, os clientes e parceiros da empresa são afetados diretamente. Consequentemente, isso pode resultar em prejuízos incalculáveis para sua organização, seja por um processo judicial por violação de privacidade ou quebra de contrato ou pelo comprometimento da sua marca perante o mercado e os consumidores.

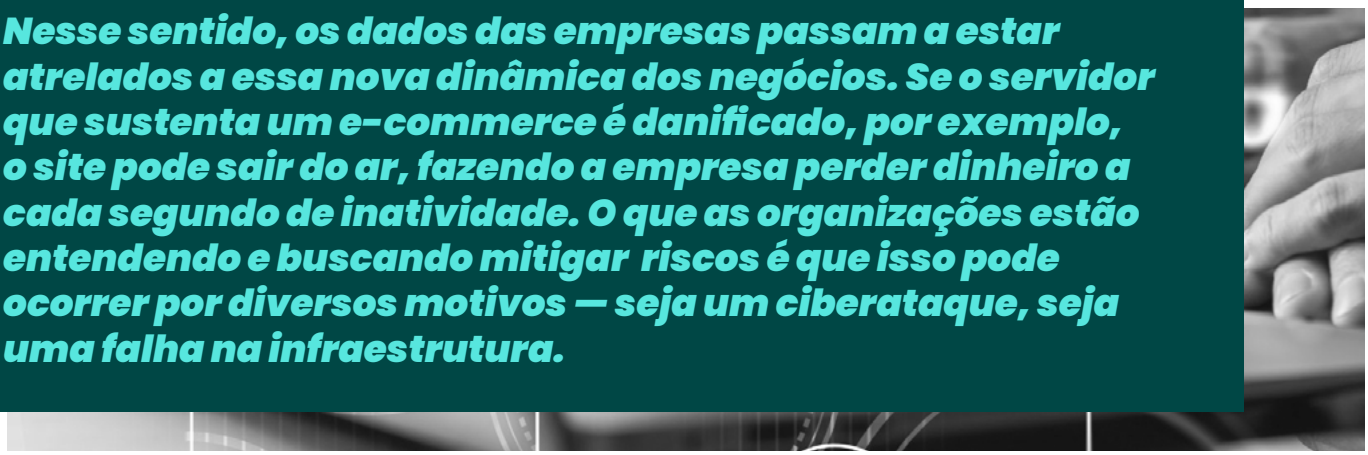
A segurança da informação nas empresas começa pela garantia de confiabilidade e confidencialidade dos dados, seja no ambiente físico, seja no digital.



COMPROMETIMENTO DA INTEGRIDADE

Com a digitalização dos negócios e o ambiente remoto se expandindo, o número de empresas que atuam 100% *online* está em constante crescimento. Mesmo setores historicamente baseados em atendimento e ambiente físico estão sendo forçados a migrar suas informações e dados para o cenário *online*.

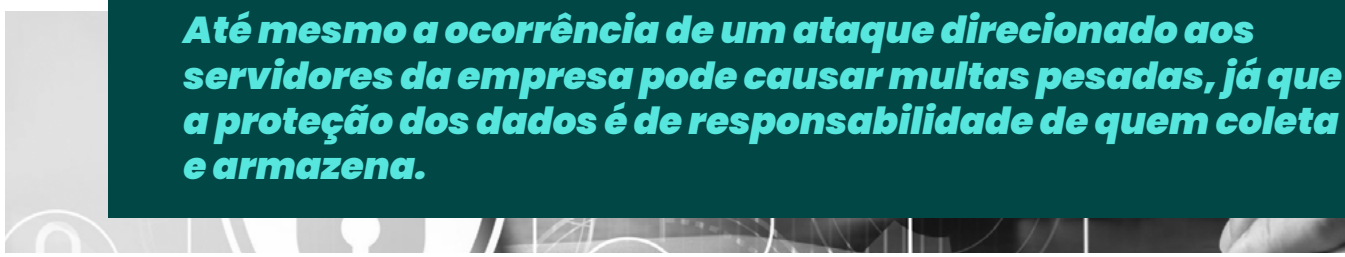
Nesse sentido, os dados das empresas passam a estar atrelados a essa nova dinâmica dos negócios. Se o servidor que sustenta um e-commerce é danificado, por exemplo, o site pode sair do ar, fazendo a empresa perder dinheiro a cada segundo de inatividade. O que as organizações estão entendendo e buscando mitigar riscos é que isso pode ocorrer por diversos motivos — seja um ciberataque, seja uma falha na infraestrutura.



RISCO DE INCONFORMIDADE

Um vazamento de dados pode ainda gerar um cenário de inconformidade jurídica. A Lei Geral de Proteção de Dados (LGPD) estabelece punições severas para quem não garantir a segurança das informações coletadas do consumidor. Por isso, toda empresa que registra dados de seus clientes deve garantir que eles não sejam repassados sem a autorização do titular.

Até mesmo a ocorrência de um ataque direcionado aos servidores da empresa pode causar multas pesadas, já que a proteção dos dados é de responsabilidade de quem coleta e armazena.

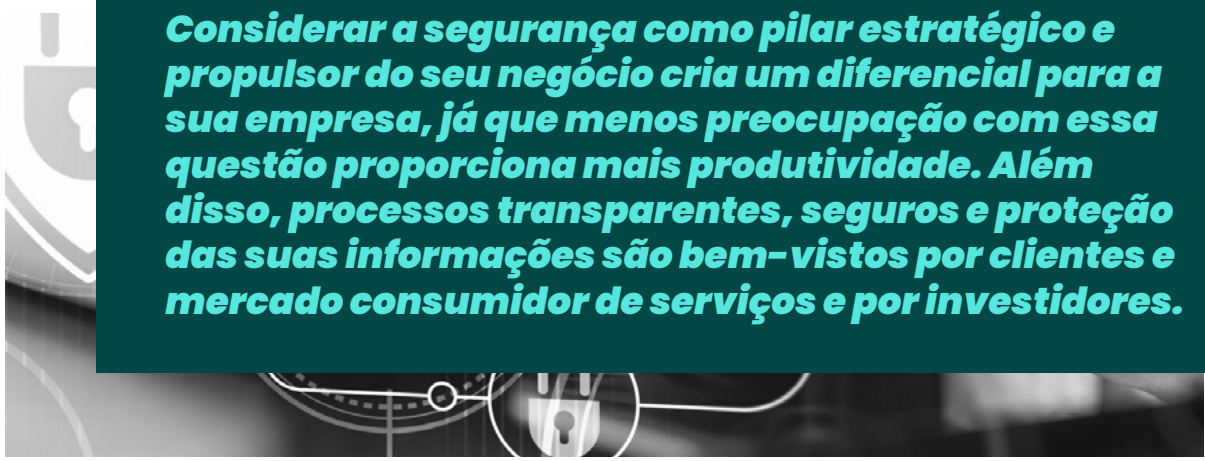


E o que podemos fazer para evitar que isso aconteça? Para começar, deve-se estabelecer uma política de segurança da informação nas empresas que considere os seus princípios básicos, sendo eles conformidade, disponibilidade, integridade, autenticidade, confidencialidade e irretratabilidade.

Tenha em mente que assunto não é de interesse apenas de grandes corporações. A LGPD é bem clara em relação à necessidade de adequação de todas as instituições (públicas e privadas) no território brasileiro.

DIFERENCIAL DE MERCADO

Considerar a segurança como pilar estratégico e propulsor do seu negócio cria um diferencial para a sua empresa, já que menos preocupação com essa questão proporciona mais produtividade. Além disso, processos transparentes, seguros e proteção das suas informações são bem-vistos por clientes e mercado consumidor de serviços e por investidores.



Nesse sentido, empresas que contam com profissionais especializados ou investem em parcerias estratégicas de confiança com vistas a assegurar o cumprimento de protocolos, boas práticas e assumem postura proativa tendem a se tornar mais resilientes – ou seja, caso venham a sofrer algum ataque, têm mais chances de se restabelecer com mais rapidez.

QUAL O PREÇO DO CIBERCRIME?

De acordo com previsões do Gartner e Julius Baer[3], a expectativa é que os gastos com cibersegurança cheguem a U$S 3 trilhões neste ano (2021). Somente no 1º semestre deste ano, o número de ataques cibernéticos a empresas brasileiras cresceu 220%, em comparação ao mesmo período em 2020 – tendo o *ransomware* (sequestro de dados) ocupado lugar de destaque como o ataque mais comum. Somente em junho, foram registrados 78,4 milhões de ataques em escala global, de acordo com relatório emitido pela SonicWall[4].

O setor de *banking* costumava ser alvo primordial dos cibercriminosos – de acordo com pesquisa realizada pela F5 Networks[5]. Entretanto, outros setores têm se tornado atrativos para os cibercriminosos. De acordo com pesquisa realizada pela IBM[6], em seu relatório global "Cost of a Data Breach Report", os três setores com o maior prejuízo advindos de um vazamento de dados são, em sequência: Saúde (U$S 7,13 MM), Energia (U$S 6,39 MM) e Financeiro (U$S 5,85 MM).

Vale ressaltar que com o advento da pandemia, o setor de saúde ganhou mais destaque e figurou nas mídias com sucessivos ataques a instituições que atuavam diretamente no combate à pandemia, como laboratórios e centros de pesquisas de desenvolvimento e distribuição de vacinas.

E por onde começar? Vejamos orientações para os setores com mais prejuízos:

SAÚDE

Adotar um modelo de segurança de confiança zero para criar sistemas e dados autodefensíveis, ao mesmo tempo em que dá suporte à conformidade com normas como a Lei Geral de Proteção de Dados (LGPD).

Documentar, comunicar e praticar um plano de resposta a incidentes em toda a empresa, incluindo participantes dos níveis de segurança, TI, jurídico, RH, relações públicas e diretoria.

ENERGIA

Adotar a análise de padrões de uso para avaliar a postura de segurança na IoT no setor (Internet das Coisas Industrial – IIoT).

Considerar a combinação da inteligência, monitoramento e operações de ameaças de segurança de TI e TO (Tecnologia Operacional).

FINANCEIRO

Minimizar a complexidade para proteger ambientes de TI e híbridos *multicloud* por meio da otimização de ferramentas e integrações de código aberto.

Impor controles rígidos de gerenciamento de identidade e acesso e aplicar os princípios de privilégio mínimo para dados e sistemas.

Essas recomendações certamente cabem em vários outros segmentos de mercado. Entretanto, antes de desenhar estratégias e propor investimento, é sempre importante considerar onde sua organização está em nível de maturidade de segurança – tanto em pessoas, processos e tecnologia, a tríade organizacional por onde a jornada de segurança da informação perpassa.

A importância da conscientização de segurança – a tão falada "*security awareness*"

É sabido que pessoas tendem a ser o elo "mais fraco" da cadeia de segurança cibernética. De acordo com pesquisa realizada pela IBM (2020)[7], o erro humano foi responsável por cerca de 95% das falhas de segurança. Corroborando com esta afirmação, temos o dado da CyberInc Insights[8] (2021), de que o erro humano tem 5 vezes mais probabilidade de causar uma violação do que outras fontes, como infraestrutura e desvios processuais, por exemplo.

A segurança da informação ainda não é uma pauta difundida nas escolas, desde o ensino fundamental. Não existe investimento em consciência de segurança do usuário como parte da educação básica, o que deveria ser primordial, considerando a massiva exposição de dados que ocorre hoje em dia, que pode ser perigosa e acarretar prejuízos para pessoas e organizações.

Os colaboradores são responsáveis por uma série de vulnerabilidades que ocorrem nas empresas, seja por estratégias mal implementadas, configurações erradas ou falta de atenção aos protocolos de segurança.

Segundo o Gartner,[9] apenas 16% dos novos contratados hoje possuem as habilidades necessárias para desempenharem suas funções atuais e futuras.

Diante disso, além de se atentar aos protocolos e investir em *softwares* e soluções de tecnologia de ponte, é urgente que as empresas invistam em treinamentos e aperfeiçoamento em relação às políticas de proteção de dados e segurança da corporação.

CONCLUSÃO

A crise instaurada pela pandemia, que impulsionou mudanças que estavam em curso na jornada de transformação digital das empresas, acendeu vários alertas no que tange ao âmbito da segurança cibernética. Com muitas organizações reformulando modalidades de trabalho para o ambiente remoto, os riscos inerentes as essas mudanças foram evidenciadas.

Realizar uma gestão segura *end-to-end*, que já era altamente desafiador em ambientes intra, tornou-se mais arriscado, pois agora o ambiente e a distribuição do negócio estão pulverizados.

As iniciativas tradicionais – testes de segurança, avaliações de riscos, avaliações de maturidade etc. – já não são mais suficientes. A segurança falha em um ponto crucial para avaliação de risco interno: o ponto de vista externo. Ciber criminosos ou *hackers* estão sempre procurando uma maneira de entrar e, para isso, se utilizam de vulnerabilidades externas detectáveis. Ou seja, olham de fora para dentro do ambiente. O "ponto de vista *hacker*" deve ser adotado, pois possibilita aos times de segurança reavaliarem as brechas expostas.

A medida que a exposição digital das organizações aumenta, cresce também a necessidade de se olhar com mais atenção os riscos, vulnerabilidades e possíveis ameaças. Muitas brechas de segurança são descobertas todos os dias possibilitando ataques criminosos, comprometendo a integridade de dados bem como a marca das organizações.

A maior efetividade da proteção do ambiente de TI está na centralização e na criação de processos e metodologias que garantam que as tecnologias estejam efetivamente protegendo os vários ativos (endpoints, redes, aplicações, nuvem etc.), que as ameaças sejam monitoradas em tempo integral (24x7x365) e os incidentes tratados de forma integrada e rápida.

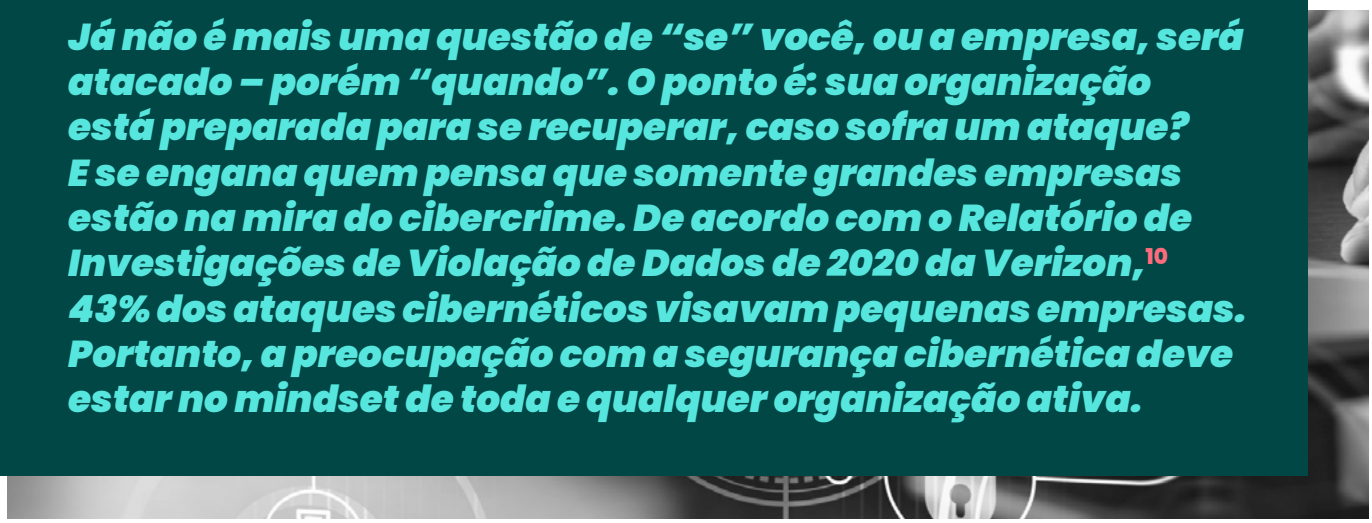
Um bom investimento é contar com um Security Operations Center (SOC) – uma solução focada em detecção e resposta a incidentes, que possibilita trabalhar a prevenção, identificação, o gerenciamento e a resolução de ameaças aos ambientes. É uma solução que conta com ferramentas como o SIEM (Correlacionador de Eventos) – que correlaciona *logs* de diversos *devices* e gera alarmes automáticos quando eventos suspeitos são detectados, além ferramentas de inteligência que monitoram redes abertas, *deep* e *dark web*.

Um SOC (Security Operations Center) é o único local capaz de monitorar e tratar em tempo real as questões de segurança da informação, de forma centralizada, dedicada e efetiva, pois em um SOC maduro, além de utilizar as melhores práticas descritas em diversos modelos de referência (NIST, ISO 27.001 etc), é lá que o CSIRT (Computer Security Incident Response Team) atua com prontidão para evitar que os incidentes gerem impactos negativos. É também lá que estão consolidados todo o conhecimento e técnicas (AI – Artificial Intelligence, SOAR – Security Orchestration

Automation and Response) para serem aplicados de forma inteligente para lidar com as ameaças.

Se sua organização está considerando evoluir sua resiliência cibernética, investir em um SOC é algo que deve estar no *roadmap* de avaliação.

Já não é mais uma questão de "se" você, ou a empresa, será atacado – porém "quando". O ponto é: sua organização está preparada para se recuperar, caso sofra um ataque? E se engana quem pensa que somente grandes empresas estão na mira do cibercrime. De acordo com o Relatório de Investigações de Violação de Dados de 2020 da Verizon,[10] 43% dos ataques cibernéticos visavam pequenas empresas. Portanto, a preocupação com a segurança cibernética deve estar no mindset de toda e qualquer organização ativa.



A estratégia é equilibrar a necessidade de proteger seus dados, ativos e ambientes com a necessidade de executar o negócio – ou seja, aumentar o seu nível de resiliência cibernética.

A boa notícia? A cibersegurança é o assunto do momento e, no mercado, existem ótimos *players* para te auxiliar nessa jornada de construção de resiliência cibernética.

Comece hoje! Considere a segurança como ponto de partida e balizadora de sucesso para sua estratégia e garanta a integridade do seu negócio.

Leidivino Natal

Leidivino Natal da Silva é CEO da Stefanini Rafael desde setembro de 2018. Possui ampla experiência em área de vendas para o mercado brasileiro e LATAM, tendo atuado em empresas multinacionais como Ericsson, Siemens e Vision-Box, auxiliando a alavancar negócios, adquirir novos clientes, ganhar mercado e mindshare por meio das atividades de marketing.

O executivo conta com grande conhecimento no mercado corporativo e de segurança da informação, atuando na definição de estratégia, posicionamento de mercado, gerenciamento de produtos, brand equity e equipes multifuncionais, priorizando o cumprimento de metas e o retorno sobre o Investimento (ROI) do negócio.

É formado em Engenharia Elétrica pela FEI (Faculdade de Engenharia de São Paulo) em 2002.

NOTAS E REFERÊNCIAS

1 Notícia: Brasil teve 3.2 bilhões de ataques online no 1º trimestre de 2021. https://www.tecmundo.com.br/seguranca/219734-brasil-teve-3-2-bilhoes-ataques-online-1-trimestre-2021.htm. Acesso em 14/09/2021

2 Gartner Top Security and Risk Trends for 2021

3 Investment Guide Outlook, Q3 2020: https://www.juliusbaer.com/fileadmin/content-hub/tendencias/investment-guide-outlook-q3-2020-es.pdf . Acesso em 14/09/2021

4 Notícia: Brasil é TOP 5 em ataques de ransomware e governo é o alvo dos Hackers.
Acesso pelo link: https://www.convergenciadigital.com.br/Seguranca/Brasil-e-top-5-em-ataques-ransomware-e-governo-e-o-alvo-dos-hackers-57672.html?UserActiveTemplate=mobile. Acesso em 14/09/2021

5 Notícia: Open Banking é principal alvo de ataque hacker no setor financeiro, diz pesquisa da F5: https://www.suno.com.br/noticias/open-banking-alvo-ataque-hacker-pesquisa/. Acesso em 14/09/2021

6 Cost of a Data Breach Report 2020; Ponemon Institute; 2020. Acesso pelo link: https://www.ibm.com/downloads/cas/QMXVZX6R. Acesso. Em 14/09/2021

7 Cost of a Data Breach Report 2020; Ponemon Institute; 2020. https://www.ibm.com/downloads/cas/QMXVZX6R. Acesso em 14/09/2021

8 Cyber Insights 2021. Cyberinc. https://cyberinc.com/thank-you-cyber-insights-report-2021/. Acesso em 14/09/2021

9 Press Release: Gartner Cautions HR and Recruiting Leaders that Only 16% of New Hires Have the Skills Needed Both for Their Current and Future Roles. https://www.gartner.com/en/newsroom/press-releases/2020-09-10-gartner-cautions-hr-and-recruiting-leaders-that-only-16-percent-of-new-hires-have-the-skills-needed-both-for-their-current-and-future-roles. Acesso em 14/09/2021

10 The 2020 Verizon Data Breach Investigations Report. https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf. Acesso em 14/09/2021