Relatório
LATAM CISO
2023

Perspectivas de CIBER-SEGURANÇA dos Líderes da Indústria

LATAM CISO

Duke UNIVERSITY

Para maiores informações, favor contatar **info@latamciso.com**

LATAM CISO Duke UNIVERSITY

Créditos

Center for Cybersecurity Policy and Law

Centro de Política e Direito de Segurança Cibernética

- Ari Schwartz
- Belisario Contreras
- Alex Botting

Duke University

- David Hoffman
- Daniel Rodríguez Maffioli
- Andy Kotz
- Sofia Bliss-Carrascosa
- Spencer Reeves

Membros da Aliança Digi Americas

aws CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google LUMU

netskope paloalto NETWORKS tenable Trellix TREND MICRO

Índice

Prefácio

David Hoffman, Profesor de Steed Family, Duke University
Andy Kotz, Investigador, Duke University
Belisario Contreras, Coordinador, Digi Americas Alliance

O Relatório de Segurança Cibernética LATAM CISO 2023 fornece informações dos líderes da indústria sobre o nível de resiliência cibernética entre várias organizações na região da América Latina. A LATAM CISO é uma rede interdisciplinar e de múltiplas partes interessadas de profissionais de segurança cibernética que visa reunir e coordenar as contribuições dos membros para estruturar as prioridades da segurança cibernética nas Américas e fortalecer sua postura geral de segurança. Este relatório foi criado para identificar lacunas de segurança, assim como as necessidades e limitações das organizações na América Latina que lhes impedem alcançar uma melhor postura frente aos ataques cibernéticos.

A região da América Latina sofre mais de 1.600 ciberataques por segundo, é imperativo que as organizações fortaleçam suas capacidades para se protegerem deste ambiente crescente de ciberataques e riscos de segurança. O relatório visa fornecer aos decisores dos setores público e privado informações para ajudá-los a compreender suas vulnerabilidades e concentrar seus esforços e recursos nas áreas dentro de seu país que mais necessitam de apoio.

Para este fim, foi realizada uma pesquisa entre os diretores de segurança da informação (CISO) e outros cargos de nível gerencial em 195 organizações diferentes setores de todos os tamanhos. Entre os entrevistados, 21% trabalha em uma organização pequena (de 1 a 100 colaboradores), 24% trabalha em uma organização mediana (de 100 a 999 colaboradores) e 56% trabalha em uma grande organização (mais de 1000 colaboradores). As indústrias mais representadas foram as de serviços financeiros (24%), governo (23%) e serviços profissionais (10%).

Mais de 70% dos entrevistados relataram que o número de ataques cibernéticos em sua organização aumentou em comparação com o ano anterior, mostrando que apesar do aumento dos esforços de segurança cibernética, os ataques persistem. O relatório começa com uma avaliação dos orçamentos das organizações, tipos de ataques, número de ataques, frequência da avaliação de risco, implementação da autenticação multi-fator (AMF), treinamento de conscientização sobre segurança e outros fatores que afetam as capacidades de segurança cibernética das organizações. O relatório conclui com um conjunto de recomendações que contribuirão para melhorar a segurança cibernética e a resiliência na região latino-americana. As recomendações concentram-se em cada categoria de coleta de dados e sugerem ações com base nos resultados. Por exemplo, os dados coletados demonstram um investimento inadequado na avaliação regular dos riscos de segurança. Um aumento nas campanhas governamentais para criar estruturas de segurança cibernética que exigem que as organizações realizem avaliações de risco mais frequentes pode permitir a identificação de vulnerabilidades.

Este relatório permitirá que as organizações examinem detalhadamente suas capacidades de segurança cibernética e compreendam os próximos passos necessários para aumentar sua resiliência frente aos ataques. De modo geral, o relatório constatou que, enquanto esforços estão sendo feitos para fortalecer as capacidades cibernéticas, as ameaças persistem. Consequentemente, as organizações devem continuar a prestar mais atenção às suas vulnerabilidades e à forma como elas podem enfrentá-las.

Como a América Latina e o Caribe podem combater os ciberataques no setor financeiro

Eric Parrado, economista-chefe, Banco Interamericano de Desenvolvimento
Diego Herrera, Especialista Líder em Mercados Financeiros, Banco Interamericano de Desenvolvimento

A região recebe mais de 1.600 ciberataques por segundo. Equipes de resposta, mecanismos de cooperação, educação formal e aumento de investimento são algumas das ações que os governos podem tomar para apoiar o setor privado na mitigação de riscos.

A América Latina e o Caribe é uma das regiões com a maior incidência de ciberataques do mundo. De acordo com dados de várias empresas de cibersegurança, a região recebe mais de 1.600 ciberataques por segundo. Para se ter uma ideia da proporção, durante os primeiros seis meses de 2022, os ataques de distribuição global de ransonware atingiram 384.000, com a região respondendo por 14% do total.[1] A correlação entre o tamanho das economias e seu nível de digitalização com o número de ciberataques é inegável: O Brasil recebe mais da metade dos ciberataques, seguido pelo México (23%), Colômbia (8%) e Peru (6%).

A cibersegurança torna-se relevante considerando que o dano econômico dos ciberataques poderia exceder 1% do produto interno bruto (PIB) em alguns países da América Latina e do Caribe. Se forem observados ataques à infra-estruturas críticas, este valor pode chegar a 6% do PIB [2] Além disso, de acordo com dados do Banco Interamericano de Desenvolvimento, 7 de 32 países pesquisados em um estudo tinham um plano de proteção de sua infra-estrutura crítica, e 20 tinham Equipes de Resposta a Emergências Informáticas (conhecidas como CERT ou CSIRT).[3]

O setor financeiro é uma infra-estrutura crítica na região. Os recentes avanços na digitalização do setor o posicionam como um dos mais relevantes em termos de cibersegurança. As cifras mostram que, após o início da pandemia da COVID-19, o número de operações financeiras através de meios digitais aumentou substancialmente na região. Por exemplo, na Colômbia, de acordo com dados da Superintendência Financeira da Colômbia, 72% das transações financeiras serão realizadas através de canais digitais, tais como telefones celulares ou internet, para 2021.[4] Além disso, segundo dados do Banco de la República (Banco Central da Colômbia), 50% dos comerciantes pesquisados adotaram canais de pagamento eletrônico.[5] Um caso emblemático é o Brasil, onde o sistema de pagamentos do Banco Central do Brasil -PIX- trata mais de 2,8 bilhões de transações por mês, 75% das quais correspondem a pagamentos de pessoa a pessoa (P2P), com a participação de quase 800 instituições que prestam serviços financeiros. Para dar uma ideia da magnitude, a PIX tem 133 milhões de usuários no Brasil. Dados de uma pesquisa

1. Informações disponíveis em: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics. Consultado em 24 de janeiro de 2023.
2. Banco Interamericano de Desenvolvimento (BID) e Organização dos Estados Americanos (OEA). 2020. "Cibersegurança": Riscos, Progresso e o Caminho a Seguir na América Latina e no Caribe". Disponível em: http://dx.doi.org/10.18235/0002513. Consultado em 24 de janeiro de 2023.
3. Ibidem.
4. Superintendência Financiera de Colombia e Banca das Oportunidades. 2022. Relatório de Inclusão Financeira (RIF) 2021. Disponível em: https://www.superfinanciera.gov.co/jsp/10111791. Consultado em 25 de janeiro de 2023.
5. Informações disponíveis em: https://www.banrep.gov.co/es/blog/efectivo-pagos-electronicos-tiempos-pandemia. Consultado em 25 de janeiro de 2023.

realizada pela empresa de cibersegurança PSafe mostraram que 844.821 tentaram atacar a infraestrutura PIX entre janeiro e junho de 2022, demonstrando a importância da cibersegurança em infraestruturas tão relevantes quanto as plataformas de pagamentos. Em outras palavras, embora a digitalização ofereça avanços significativos no campo da inclusão financeira, também apresenta desafios em termos de cibersegurança.

A grande vantagem do setor financeiro é que ele é um dos mais organizados em termos de cibersegurança na região. De uma perspectiva pública, as autoridades financeiras em países como o Chile assumem riscos operacionais em infraestruturas do setor financeiro como um componente da análise de estabilidade financeira. A participação de várias entidades (ministérios das finanças, bancos centrais, superintendências e comissões bancárias, de títulos, pensões e seguros, entre outros) em grupos colegiados, como os conselhos de estabilidade financeira, proporciona flexibilidade para gerar políticas públicas e mudanças regulatórias que mitigam os riscos cibernéticos nas jurisdições da região. De uma perspectiva privada, mostra como o setor coopera em nível regional para compartilhar informações sobre incidentes de ciberataques em nível individual das entidades do setor. O papel das associações regionais, como a Federação Latino-Americana de Bancos (FELABAN), é importante para consolidar este tipo de esforços e para ter bases de dados de incidentes.

Recomendações para combater os ciberataques no setor financeiro

Para combater os ciberataques, é aconselhável tomar medidas de política pública para orientar ao setor privado na mitigação dos riscos. As três recomendações básicas são as seguintes. Inicialmente, recomenda-se a criação de uma equipe nacional de resposta a incidentes de cibersegurança (CSIRT) para melhorar os níveis de preparação e resposta aos ciberataques.

Em nível nacional, é útil gerar bancos de dados de incidentes informáticos para infraestruturas chave, como as do setor financeiro, e gerar políticas que favoreçam o intercâmbio dinâmico de informações sobre incidentes entre entidades e setores. É também essencial que os CSIRTs nacionais pertençam a plataformas como CSIRT Américas, que permitem o compartilhamento de informações e gerar mecanismos de cooperação em nível regional. O setor financeiro deve fazer parte dessas iniciativas. Da mesma forma, é necessário treinar funcionários das entidades financeiras e públicas do setor. A educação deve ser acompanhada de uma constante atualização de tendências e tecnologias para mitigar os riscos cibernéticos. Finalmente, estas duas questões devem ser acompanhadas de investimentos em tecnologia para mitigar os riscos da cibersegurança e sua materialização. Estima-se que o setor financeiro da região gasta 10% de seu orçamento tecnológico com este tópico relevante. À medida que o setor se torna mais digitalizado, mais investimentos podem ser necessários.

Em conclusão, a formalização do CSIRT, mecanismos de cooperação nacional e internacional, educação formal e investimento em cibersegurança permitirão que nossos setores financeiros mitiguem os riscos associados a um negócio mais digital com vocação de proteção ao consumidor.

Cibersegurança e o Setor Financeiro na América Latina e Caribe

Giorgio Trettenero Castro, Secretário Geral da Federação Latino-Americana de Bancos (FELABAN)

A Federação Latino-Americana de Bancos (FELABAN) nasceu como um representante dos bancos latino-americanos para aderir a um dos mais altos padrões de cibersegurança na região. A FELABAN, com foco específico em cibersegurança e fraude bancário, visa melhorar a eficiência e a estabilidade do sistema financeiro latino-americano, bem como a capacidade de cibersegurança na região como um conjunto.

Vemos a comunicação e a colaboração, ou melhor, a falta dela, como uma das maiores ameaças ao cenário da cibersegurança. A medida que os bancos se transformam em um ambiente mais digital, os mecanismos de quebra de segurança e fraude evoluem em paralelo. Enquanto um banco, ou um país, pode compreender estas novas ameaças, o resto da região precisa de tempo para se recuperar e muitas vezes o faz quando é tarde demais.

FELABAN, com o objetivo de formar fortes conexões regionais e cumprir sua missão como união bancária, tomou a iniciativa de desenvolver um projeto inovador de colaboração latino-americana que visa construir pontes entre bancos em toda a região e formar uma linha aberta de comunicação. Ao compartilhar as melhores práticas e informações-chave sobre segurança bancária, bancos de 11 países diferentes foram capazes de mitigar os riscos inerentes às operações financeiras do dia-a-dia. Este projeto piloto, que começou em outubro de 2022 e terminou em janeiro de 2023, é baseado em um novo modelo de colaboração e abre caminho para o intercâmbio de informações entre os bancos da região.

Os resultados preliminares deste piloto foram excepcionalmente positivos: uma nova dinâmica de compartilhamento de informações mostrou aos bancos envolvidos a capacidade de resposta que podemos alcançar trabalhando juntos, e ainda há muito espaço para crescimento. As instituições estão compartilhando informações relevantes que estão mudando a maneira como elas enxergam a segurança bancária. Um caso de fraude ou um ataque não é mais um evento isolado. Devido a este aumento do nível de intercâmbio, encontramos padrões em diferentes casos de fraude, mesmo entre países. Certas técnicas de fraude dependem de vários canais de interação entre os países. Aumentando a comunicação e trabalhando para compreender a fraude no país de outro, a resposta à fraude em seu próprio país pode ser melhorada.

Se olharmos para o futuro, esperamos incorporar ativos tecnológicos mais fortes em nossos projetos regionais. Sob a dinâmica atual deste modelo colaborativo, acreditamos que compartilhar certas tecnologias será fácil e eficaz. Ao implementar um modelo colaborativo que alavanca a tecnologia atual e a inteligência artificial, podemos capacitar um banco ou país a se defender rapidamente contra uma violação cibernética. Esta solução aumentará as capacidades de cibersegurança e fornecerá uma resposta mais eficiente e eficaz às ameaças potenciais.

Ao continuarmos a analisar os dados deste projeto piloto inicial, com foco na LATAM, estamos extremamente otimistas quanto ao seu potencial. Como região, a América Latina enfrenta muitas ameaças semelhantes, se não exatamente as mesmas. Com a formação de um grupo coletivamente responsável, o setor financeiro, ou qualquer indústria, fortalecerá suas capacidades de cibersegurança coletiva, bem como sua capacidade de responder a ataques e crescer no futuro.

O CISO como Narrador Empresarial? Obtendo a Atenção da Diretoria

Seán Doyle, Lead, Centro de Cibersegurança, Fórum Econômico Mundial

Em fevereiro de 2022, um ciberataque aos serviços comerciais via satélite na Ucrânia causou a falha de parques eólicos geradores de energia elétrica em toda a Europa Central. Pouco mais de seis meses antes, em julho de 2021, os supermercados na Suécia foram obrigados a fechar suas portas após um ciberataque a um provedor de serviços de TI sediado na Flórida, EUA, perturbando as operações de seus clientes internacionais. Em ambos os casos, o fluxo contínuo de perturbações não foi previsto nem previsível. O primeiro alvo desses ataques foram os prestadores de serviços compartilhados. Eles não eram nomes familiares e não pareciam ter um papel importante e um ponto de vista sistêmico no ecossistema digital. No entanto, as consequências se estendem através de setores e fronteiras.

Estes incidentes mostram como as diferentes tecnologias em uma multidão de organizações têm agora as mesmas dependências ou fraquezas em comum. Isto significa que o impacto dos incidentes de cibersegurança pode passar de uma organização para outra e através das fronteiras. Os riscos que isto cria são sistêmicos, contagiosos e muitas vezes ultrapassam a compreensão ou controle de qualquer entidade individual. Os riscos sistêmicos podem ser difíceis de prever e quantificar, e ainda mais difíceis de administrar. O ambiente de ameaça se tornou mais volátil e os ataques têm maior potencial disruptivo. As organizações devem dividir sua atenção entre a defesa contra ataques cibernéticos e a resiliência após a ocorrência de um ataque cibernético.

Tente colocar-se no lugar das equipes de segurança da empresa de eletricidade e da cadeia de supermercados que foram "danos colaterais" dos ataques discutidos acima. O que eles poderiam ter feito para evitar esta interrupção? A resposta mais provável é "não muito". Muitas dependências tecnológicas são agora difíceis de serem vistas até que sejam quebradas. Não podemos evitar o que não podemos ver. Isto significa que é necessário prestar mais atenção à resiliência e à capacidade de se recuperar de ataques ou reduzir os danos que eles podem causar.

A pesquisa do Fórum Econômico Mundial, que será publicada integralmente em seu relatório Anual de Perspectivas Cibernéticas em 2023, também encontrou uma tendência positiva. As diretorias estão mais conscientes do que nunca dos riscos cibernéticos. Isto se deve em parte a ataques de alto perfil em todos os setores. A agitação geopolítica na Europa também trouxe a questão da segurança cibernética para as mesas de café dos membros da diretoria, já que a ameaça da guerra cibernética faz manchetes em todo o mundo. As diretorias também estão sendo atraídas para a questão por um corpo crescente de regulamentação e pelo desenvolvimento de princípios aceitos para a governança de risco de segurança cibernética nos altos níveis da administração. Isto ajuda a concentrar a atenção nos benefícios de integrar a resiliência cibernética nos processos comerciais e nas estruturas de governança. Seja qual for a razão, o aumento do foco no risco cibernético a nível da diretoria é uma oportunidade para os CISO em 2023.

O que o CISO pode fazer?

As diretorias estão pronta para ouvir suas equipes de segurança cibernética. Os CISO bem sucedidos podem explicar o risco cibernético de uma forma que faça sentido para a diretoria. Eles tornam a história da segurança cibernética acessível aos executivos e traduzem o risco cibernético em métricas, tais como

ganhos e perdas operacionais ou danos à reputação, que os executivos empresariais entendem e podem usar para priorizar os gastos.

Começar sua história com a situação geopolítica pode ser um bom ponto de entrada para explicar por que sua organização pode ser atacada por criminosos ou como pode ser afetada por ataques prejudiciais a outras organizações. Mostrar aos líderes empresariais como seria concretamente um risco cibernético abstrato em seu negócio permite às diretorias entender o significado de um ataque cibernético, mas também distribuir a responsabilidade pela resiliência cibernética além da equipe de segurança da informação para as unidades comerciais.

Em termos de recursos, o apoio nos altos níveis de gestão facilita a integração da governança de risco cibernético em toda a organização. Se a diretoria estiver interessada na resiliência cibernética, o resto do negócio seguirá. Isto pode tornar a organização um ativo para a equipe do CISO e não apenas um alvo a ser defendido. Nossa pesquisa indicam que as diretorias provavelmente se sentirão mais confiantes na segurança de suas organizações quando o gerenciamento do risco cibernético for integrado à tomada de decisões e processos em todas as suas organizações. Por exemplo, algumas das empresas pesquisadas para o relatório Global Cyber Outlook 2023 incluem o CISO ou membros de sua equipe em órgãos-chave, tais como comitês de auditoria, de risco e finanças. Nestes casos, o CISO e sua equipe se tornam assessores de confiança para as equipes comerciais e apoiam o desenvolvimento seguro de novos processos comerciais.

As empresas estão mudando a maneira como utilizam a tecnologia. Isto cria dependências tecnológicas invisíveis e novos riscos cibernéticos. O papel do CISO não será menos complicado tecnicamente em 2023. Entretanto, as oportunidades para engajar os líderes empresariais na questão da gestão de riscos cibernéticos estão aumentando.

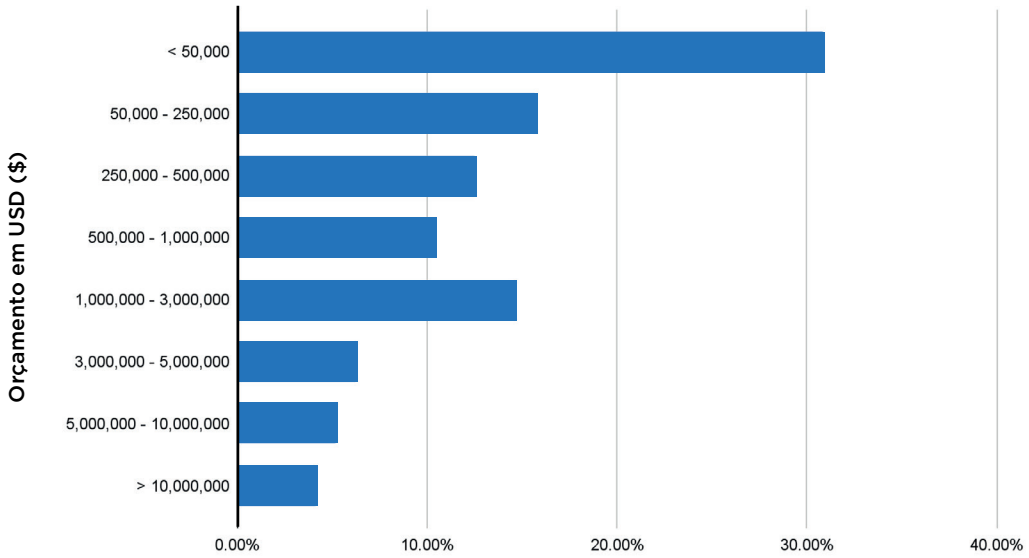

.fcb-popup {
position: absolute;
top: 0;
left: 0;
width: 100%;
height: 100%;
z-index: 10;
}

Achados

Orçamento dedicado à **Cibersegurança**

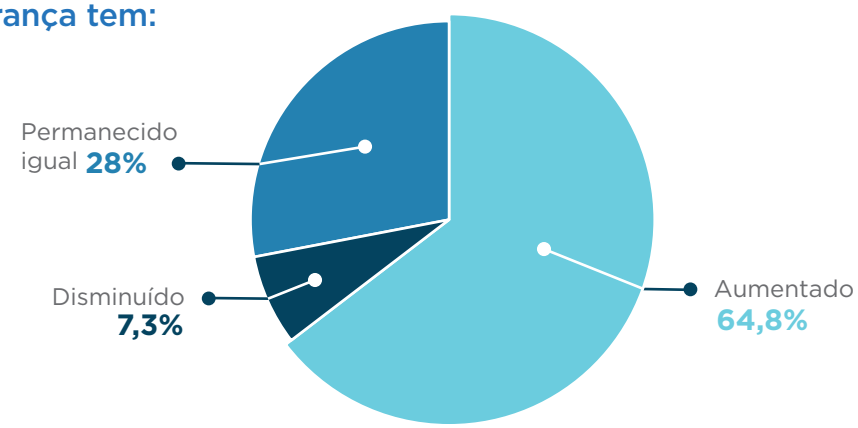
Com relação ao orçamento para segurança cibernética dentro da organização, 31% dos entrevistados relatam ter um orçamento de menos de $50.000 (USD), e a maioria (59%) das organizações tem um orçamento de menos de $500.000. O orçamento de segurança cibernética tinha aumentado para 65% dos entrevistados em comparação com o ano anterior, e o orçamento tinha diminuído para apenas 7%. Isto mostra uma compreensão crescente da importância da cibersegurança entre estas empresas.

Q5. Orçamento de Cibersegurança



Em particular, a maioria das organizações com um orçamento de segurança cibernética inferior a $ 50.000 dólares não viu um aumento em seu orçamento de segurança cibernética, mas permaneceu igual e, em alguns casos (8,47%), seu orçamento de segurança cibernética diminuiu. Dado que o grupo de entrevistados com orçamentos inferiores a $ 50.000 é o maior da pesquisa, e que a maioria dessas empresas viu um aumento nos ataques cibernéticos no último ano, valeria a pena identificar as razões que explicam a estagnação do orçamento, a fim de abordar efetivamente essas causas no futuro.

Q6. O orçamento da cibersegurança tem:

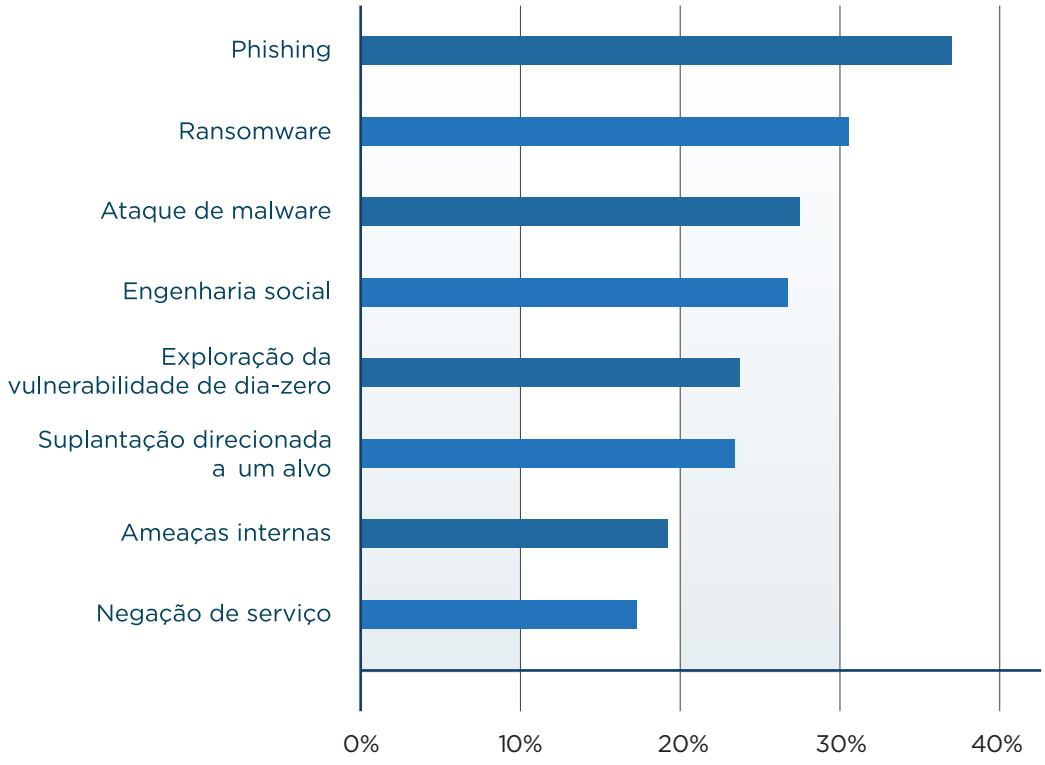


ACHADOS

Tipos de ciberataques enfrentados

- Entre as inúmeras formas de ataques cibernéticos, ataques de phishing (roubo de identidade), ransomware (sequestro de arquivos para resgate) e malware (software malicioso) são alguns dos mais comuns. Ao compreender os tipos mais comuns de ataques, as equipes de segurança cibernética podem combatê-los de forma mais eficiente. As categorias de ataques frequentemente se sobrepõem (phishing e engenharia social), mas comparar as classificações das respostas ajuda a entender o que mais preocupa aos CISOs. Quando a pesquisa pediu classificar os cinco principais tipos de ataques de acordo com o que ocorre com mais frequência, 37% dos entrevistados classificaram o phishing como o número 1, e 98% dos entrevistados o escolheram dentro do top 5. As próximas respostas mais comuns classificadas como número 1 foram ataques de resgate e malware, com 31% e 28% respectivamente. Além disso, 95% dos entrevistados classificaram estes dois como os 5 primeiros.
- Curiosamente, a engenharia social, uma das únicas formas "não técnicas" de ataque, foi classificada como número 1 por 27% dos entrevistados e no top 5 por 95%. Isto destaca a importância não só das defesas técnicas de segurança cibernética, mas também de garantir uma boa higiene cibernética entre os funcionários.
- Outras formas notáveis de ataques mencionados como número 1 são vulnerabilidades de segurança de dia zero (24%), phishing direcionado (24%), negação de serviço (DoS) (17%) e ataques baseados em IoT (17%), entre outros.

Q7. Os tipos mais comuns de ataques cibernéticos



ACHADOS

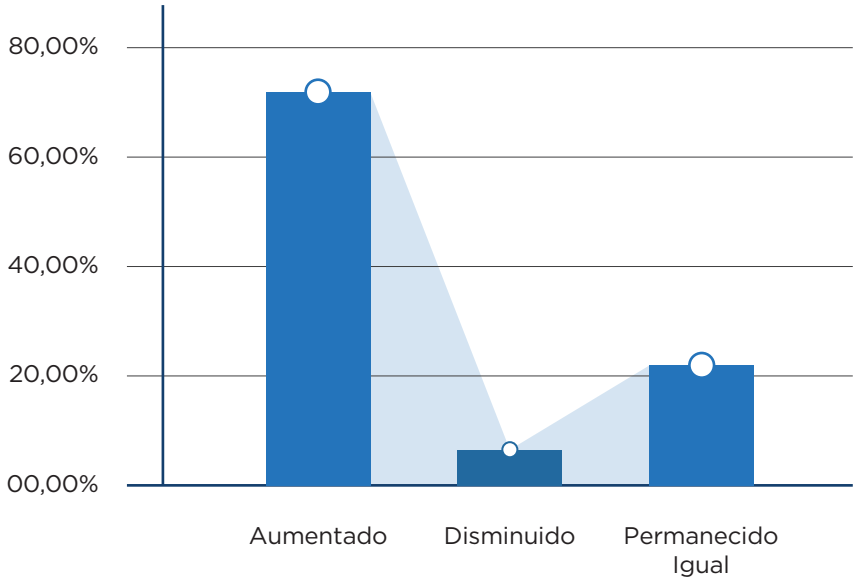
Ataques cibernéticos ano após ano

- Mais de 71% dos entrevistados relataram que o número de ataques a sua organização havia aumentado desde o ano anterior. Apenas 8% dos entrevistados relataram uma diminuição no número de ataques. Com este grande aumento em tão curto período de tempo, a importância das avaliações de risco de segurança, treinamento de funcionários e outros esforços cibernéticos relacionados à segurança cresceu exponencialmente.

- Mais da metade dos respondentes em todos os setores considerados, com exceção da agricultura e da mineração, e dos setores de mídia e entretenimento, observaram um aumento nos ataques. Para os setores de informática e eletrônicos, bens de consumo, manufatura, viagens e hospitalidade e varejo, cada um dos entrevistados relatou um aumento nos ataques em comparação com o ano passado, indicando a necessidade desses setores específicos melhorarem suas defesas de segurança cibernética.

- Mais organizações grandes do que as médias ou pequenas (78% comparado a 61% e 63% respectivamente) perceberam um aumento no número de ataques, refletindo como as grandes organizações são frequentemente um alvo preferencial para os cibercriminosos. Uma razão para isso poderia ser a maior visibilidade, mas também as maiores consequências de um ataque contra grandes empresas, que serve como alavanca para que os criminosos atinjam seus objetivos. Outra razão possível para esta diferença é que organizações menores com orçamentos menores podem não priorizar o monitoramento do número de ataques.

Q8. Mundança nos ataque desde ano anterior

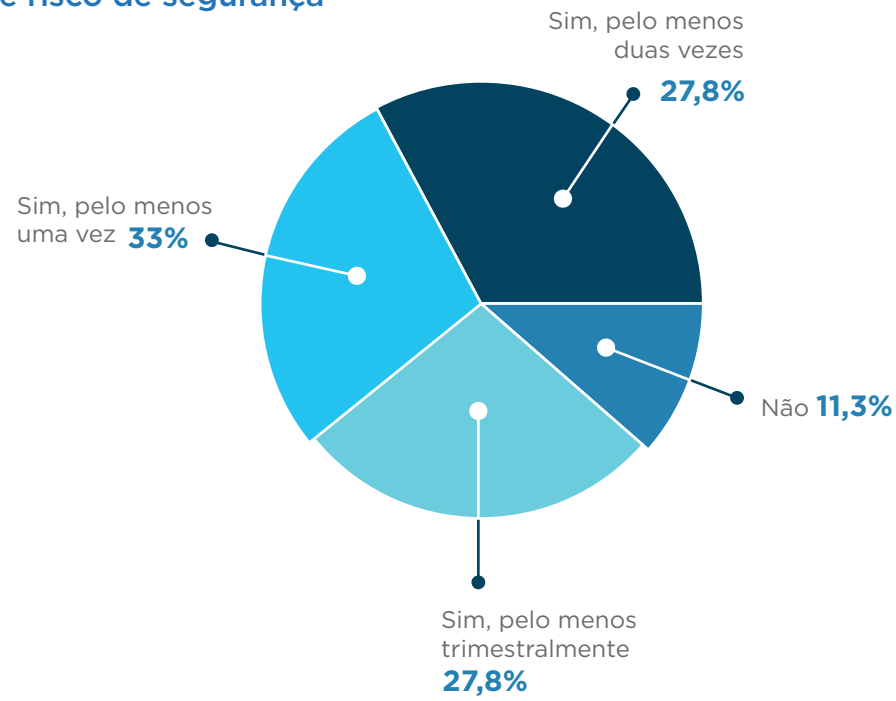


ACHADOS

Frequência da avaliação de risco de segurança

- Muitas organizações levam a sério a crescente ameaça de ataques de dia zero e ainda há espaço para o crescimento. Mais da metade de todas as organizações (60,83%) realizam avaliações de risco de segurança apenas "pelo menos uma vez por ano (33%)" ou "pelo menos duas vezes por ano (28%)". Apenas 28% das organizações realizam estas avaliações pelo menos trimestralmente. Dada a frequência e a natureza oculta dos ataques de dia zero, avaliações regulares de segurança são críticas para identificar novas vulnerabilidades de dia zero e impedir a exploração.
- Embora o foco dos ataques de dia zero varie ligeiramente entre as indústrias, dois setores em particular têm destaque. Em particular, 66,67% dos entrevistados de organizações sem fins lucrativos relataram não ter realizado avaliações de risco de segurança nos últimos 12 meses, embora as organizações sem fins lucrativos estejam igualmente expostas a ataques cibernéticos como empresas privadas ou entidades públicas.
- No entanto, 40% dos entrevistados no setor de saúde não realizaram avaliações de segurança. O setor de saúde é particularmente propenso a ciberataques devido à sensibilidade e ao valor dos dados dos pacientes que coleta.

Q9. Frequência da avaliação de risco de segurança

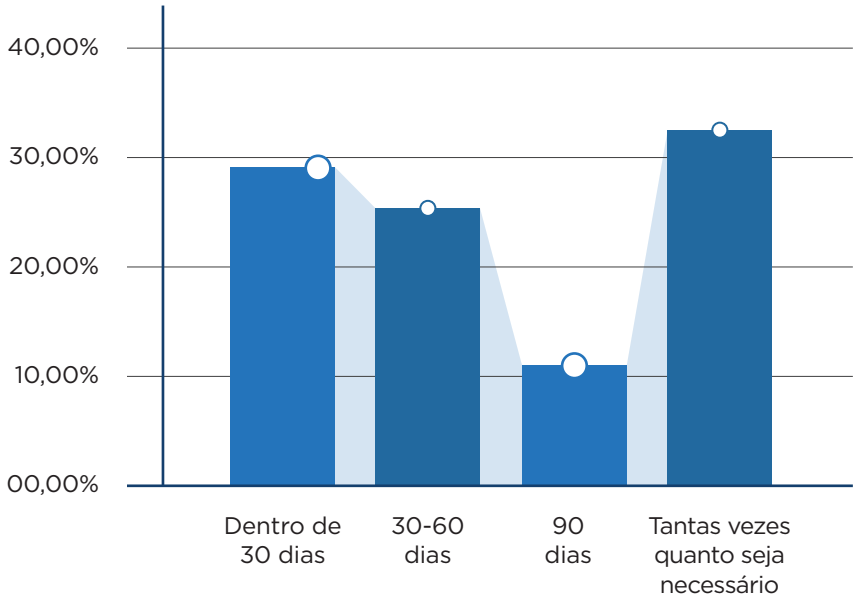


Frequência de patches de segurança

- A maioria dos remendos foi aplicada em 30 dias (29%) ou 60 dias (26%). Outros 34% também afirmaram que aplicaram patches "tantas vezes quanto necessário". Além dos patches de segurança da própria organização, 65% relataram ter aplicado patches em aplicações de terceiros. As empresas tendem a confiar em fornecedores de software e aplicativos de terceiros para gerenciar suas operações. Essas aplicações geralmente exigem atualizações de segurança regulares, de modo que não serão usadas como vetores para obter acesso aos sistemas da empresa.

- Curiosamente, as organizações com o menor orçamento de cibersegurança ($0-$50.000) tinham menos probabilidade de remendar aplicações de terceiros, sendo que apenas 48,28% delas o faziam. Isto torna necessário avaliar se existe uma correlação entre os baixos orçamentos das organizações e sua capacidade para aplicar os patches. Uma explicação possível é que as organizações menores não têm os recursos técnicos e humanos para reconhecer quando os patches são necessários e/ou não têm os recursos para instalá-los.

Q10. Frequência de patches de segurança

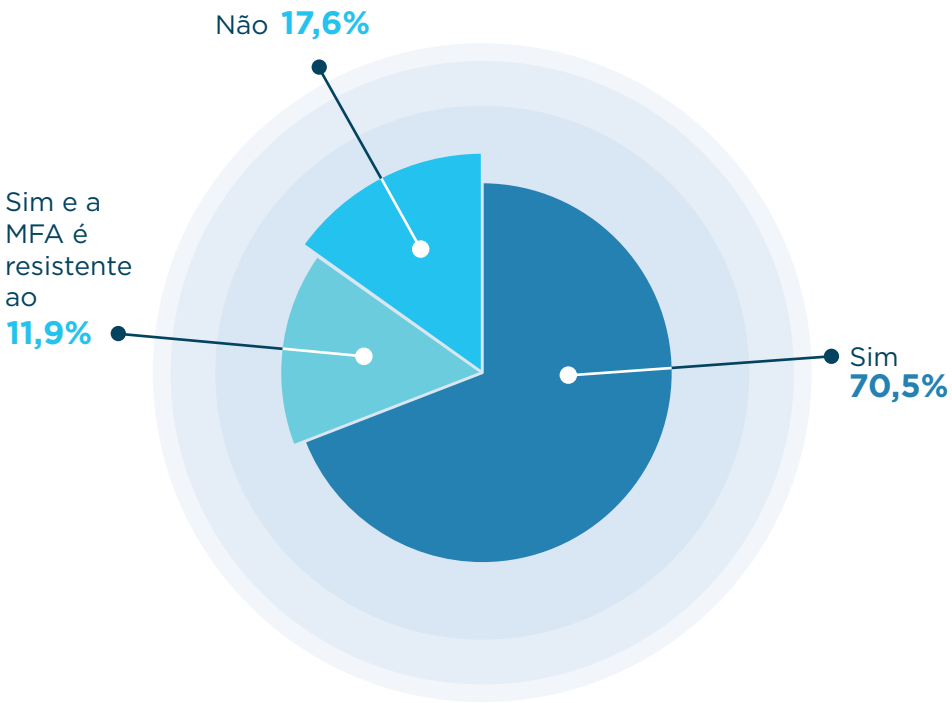


ACHADOS

Implementação de autenticação multi-fator

- Uma das maneiras mais fáceis de prevenir, ou pelo menos mitigar, possíveis ataques cibernéticos é proteger melhor o login e o acesso às informações dos funcionários. O uso da AMF é uma das melhores táticas para isso, pois ajuda a garantir que um usuário autorizado acesse as informações, em vez de um ator externo. Vale a pena salientar que 70% das organizações dos respondentes implementam alguma forma de AMF, e outros 12% implementam AMF resistente ao phishing (como FIDO ou PKI).
- Surpreendentemente, as grandes organizações foram as mais propensas a não implementar a AMF, com 19% relatando que o fizeram. Isto é cerca de 2 pontos acima da média, com apenas 13% das pequenas organizações relatando que não implementam a AMF.
- As organizações com orçamentos entre US$ 250.000 e US$ 500.000 (96%) tinham maior probabilidade de implementar alguma forma de AMF.

Q12. A implementação da AMF

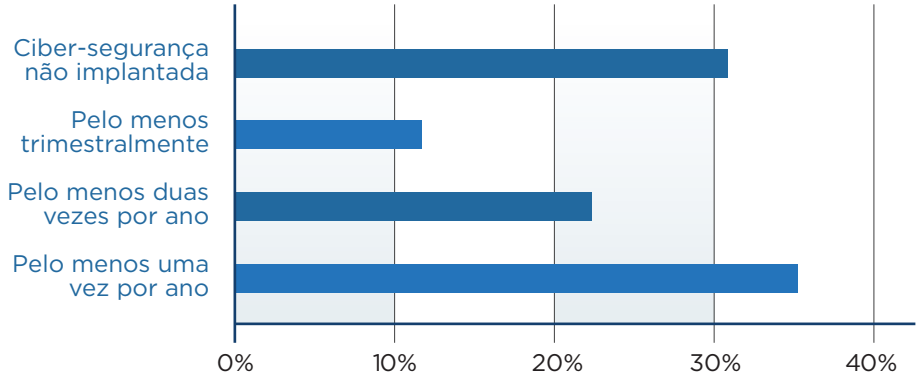


ACHADOS

Frequência dos exercícios de simulação

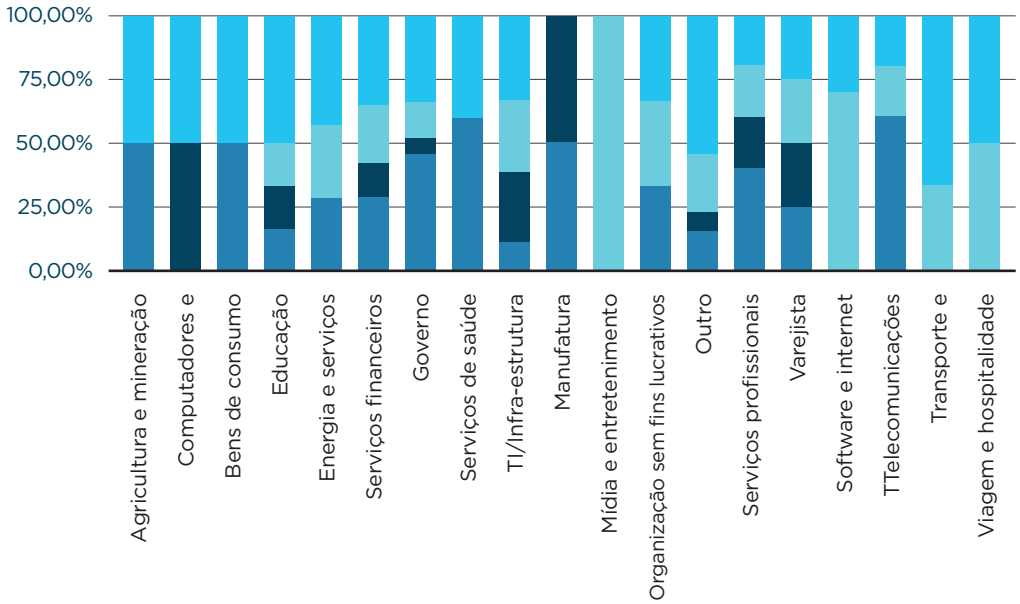
- Outras formas de preparação são igualmente importantes, tais como exercícios de simulação de segurança cibernética e treinamento de conscientização de segurança para funcionários. 30% de todos os entrevistados relatam que sua organização não realiza exercícios de simulação de ciber-segurança. Outros 35% relatam que realizam tais exercícios "pelo menos uma vez por ano". Para estarem mais bem preparadas para a resposta a incidentes, as organizações devem se preparar para tais exercícios com mais frequência.
- Algunos setores informam que não conduziram exercícios de simulação de cibersegurança mais do que outros. Enquanto em média 30% das organizações relatam não ter realizado tais exercícios, certas indústrias relatam taxas muito mais altas, como por exemplo: Saúde (60%), Serviços Profissionais (40%), Telecomunicações (60%) e Governo (46%). Todos esses setores relataram um aumento percebido no número de ataques no último ano.
- Pequenas organizações (39%) e organizações com orçamentos inferiores a 500.000 dólares por ano também informam que não realizaram exercícios de simulação, muito provavelmente devido à falta de recursos.

Q15. Frequência dos exercícios de simulação



Q15. Frequência de exercícios de simulação por indústria

- 4. Pelo menos uma vez por ano
- 3. Pelo menos duas vezes por ano
- 2. Pelo menos trimestralmente
- 1. Nenhum exercício(s) de ciber-segurança foi/foram realizado(s)

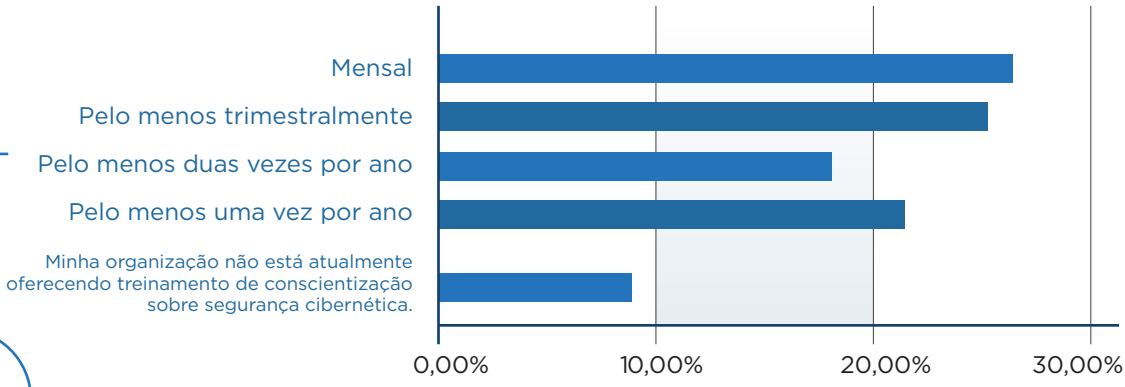


ACHADOS

Treinamento de conscientização de segurança

- Mais de 50% dos entrevistados relataram que fornecem treinamento de conscientização de segurança mensalmente (26%) ou trimestralmente (25%), e outros o fazem pelo menos duas vezes por ano (18%) ou uma vez por ano (22%). Apenas 8% relatou uma total falta de treinamento de conscientização de segurança.
- Havia pouca variação entre tamanho ou indústria, com exceção das pequenas organizações, que não forneciam treinamento com a mesma frequência que as médias e grandes empresas.

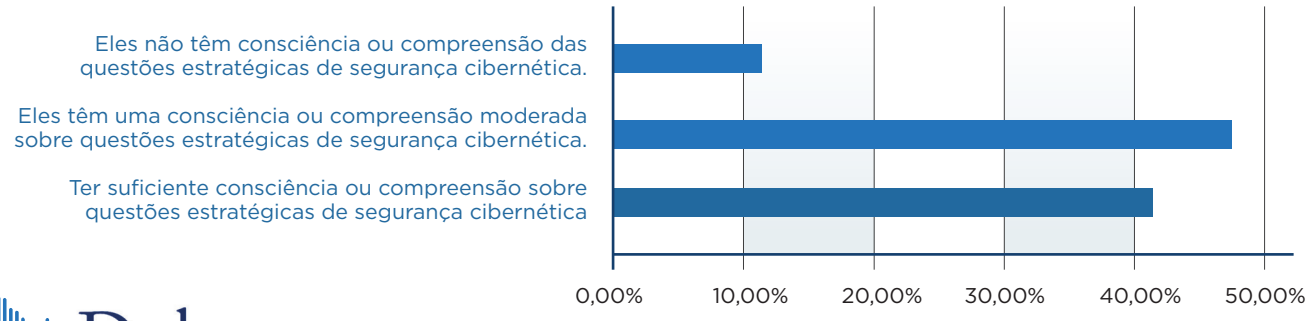
Q16. Frequência do treinamento de conscientização de segurança



Confiança nos executivos de nível C

- Quando perguntados sobre executivos de nível C, 47% dos entrevistados acreditavam que esses executivos tinham "consciência moderada e conhecimento de questões estratégicas de cibersegurança" e 41% acreditavam ter "consciência suficiente...". Além disso, 11% dos entrevistados acreditavam que seus executivos de nível C "não têm conhecimento e compreensão das questões estratégicas de segurança cibernética". Os executivos de nível C devem se esforçar para estar bem informados sobre as estratégias de segurança cibernética, ou assegurar que aqueles ao seu redor o estejam.
- As organizações menores tinham um pouco menos de confiança em seus executivos, mas as diferenças eram mínimas entre tamanho, orçamento e indústria.

Q13. Confiança na Diretoria e nos Executivos de nível C

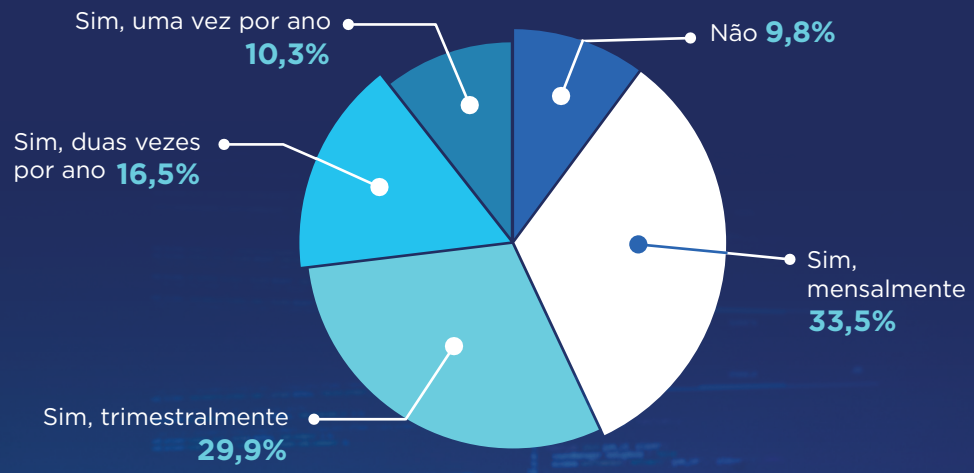


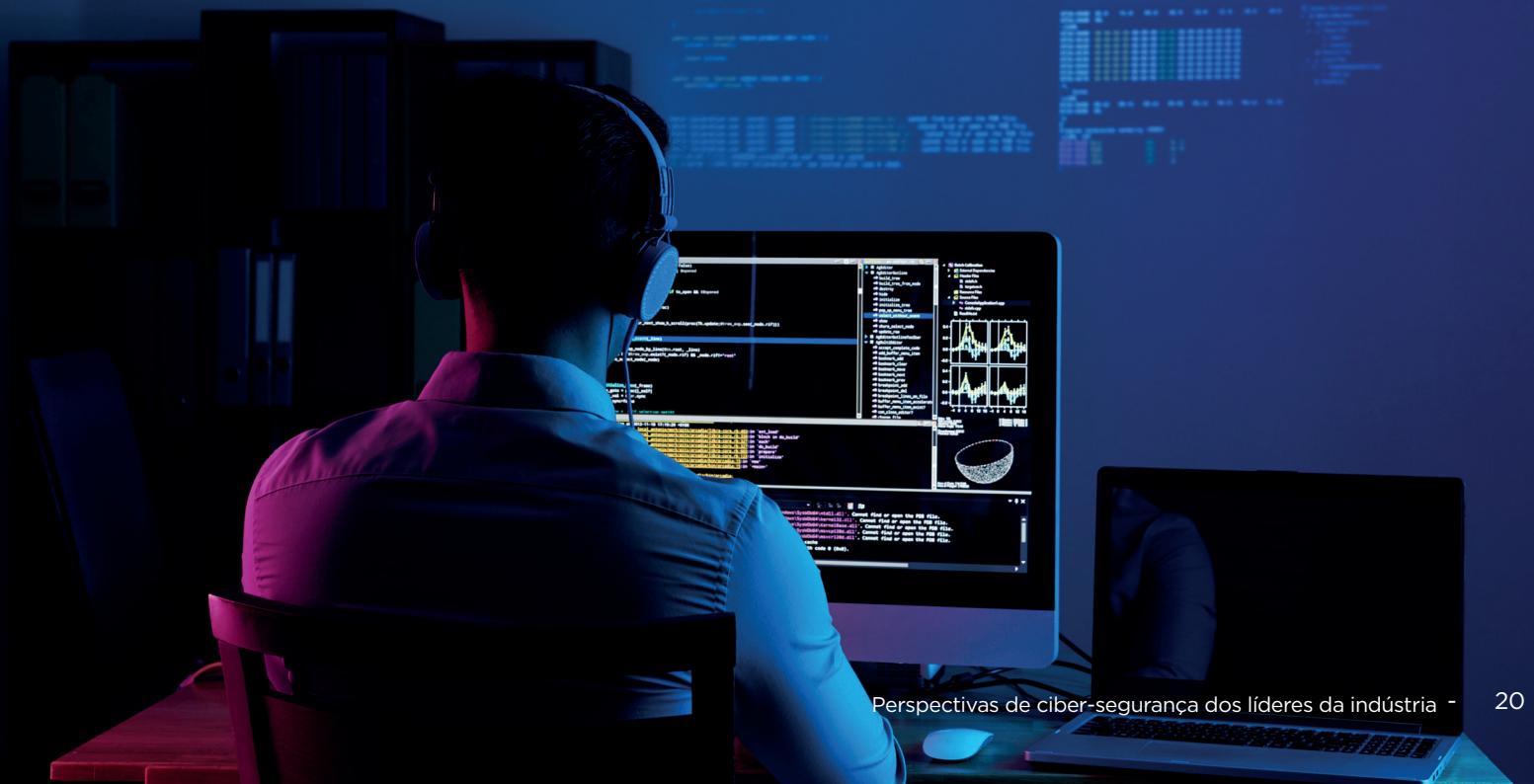
ACHADOS

Frequência do relatório de ciber-segurança

- Muitas organizações forneceram relatórios para a diretoria e executivos de nível C sobre o estado da segurança cibernética. Mais da metade das organizações dos respondentes forneceram relatórios mensais (34%) ou trimestrais (30%), com mais 17% emitindo relatórios duas vezes por ano e 10% emitindo relatórios uma vez por ano. Apenas 10% das organizações não forneceram relatórios de segurança cibernética.

Q14. Frequência dos Relatórios aos Diretores e ao Grupo C



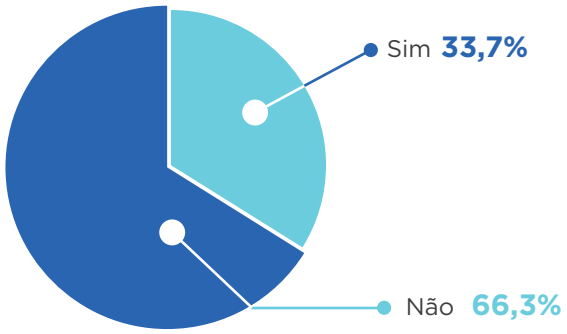


ACHADOS

Seguro de Responsabilidade Civil Cibernética

- Em termos de outras formas de preparação e resposta a incidentes cibernéticos, mais de 66% dos entrevistados relataram que sua organização não possuía nenhuma forma de seguro de responsabilidade civil cibernética. O seguro de responsabilidade civil é outra medida da vontade dos executivos de investir em segurança cibernética.
- Em particular, 85% das pequenas organizações não possuíam seguro de responsabilidade civil cibernética. Para melhorar sua posição de resiliência, é crucial que as organizações menores trabalhem com o mesmo empenho para prevenir e mitigar os danos.
- As empresas com o orçamento mais baixo tinham menos probabilidade de obter um seguro de responsabilidade civil, indicando que um orçamento baixo pode ser uma das principais barreiras ao acesso a ele.

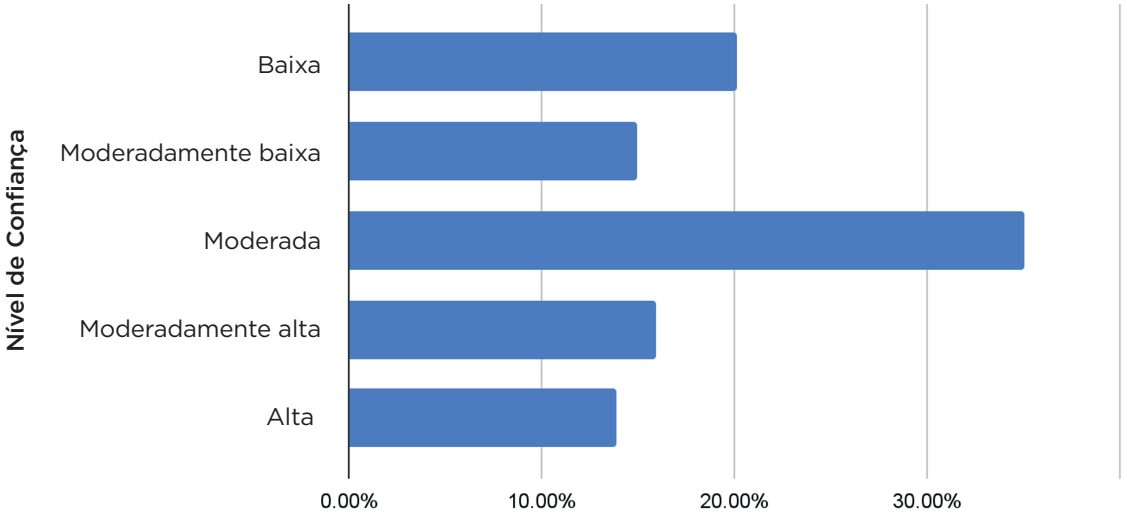
Q17. Seguro de Responsabilidade Civil Cibernética



Agências Nacionais de Aplicação da Lei e CERTs Nacionais

- Após um ataque cibernético ou incidente cibernético relacionado, as organizações devem entrar em contato com as agências nacionais de aplicação da lei e/ou a CERT nacional. Embora a maioria das organizações esteja ciente dos procedimentos adequados para isto, 32% relataram que não sabiam quem contatar ou como contatá-los.
- Com relação ao apoio nacional para respostas a ataques cibernéticos, 35% das organizações tinham baixa (20%) ou moderadamente baixa (15%) confiança nas agências nacionais de aplicação da lei e em sua CERT nacional. Outro 35% relatou uma confiança moderada nas mesmas agências, com apenas 16% relatando confiança alta a moderada e 14% relatando alta confiança.
- Organizações sem fins lucrativos (67%) e de telecomunicações (60%), assim como pequenas organizações, relataram os níveis mais baixos de confiança.
- A capacidade de trabalhar cooperativamente com governos e agências governamentais após um ataque cibernético ou incidente cibernético relacionado é fundamental para prevenir outros crimes similares.

Q18. Confiança nas Agências Nacionais de Aplicação da Lei e CERT

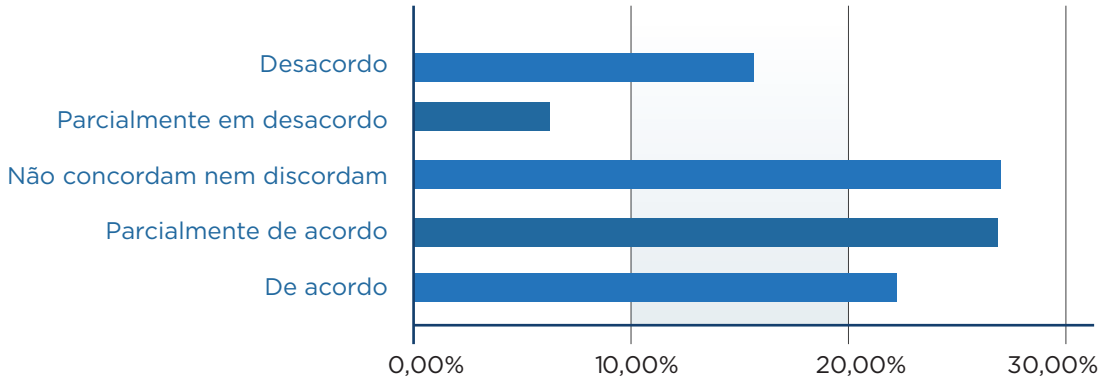


As entradas são levadas em conta para a política pública, regulamentação, etc.

- Uma explicação possível para a falta de confiança nas agências nacionais de aplicação da lei e nos CERTs é que as organizações não sentem que sua contribuição é levada em consideração no desenvolvimento de políticas públicas, regulamentos e outras iniciativas com impacto nacional. Quando perguntados se a contribuição de sua organização foi levada em consideração, 23% dos entrevistados estiveram parcialmente em desacordo, e 28% dos entrevistado não concordaram nem discordaram. Aproximadamente 50% das organizações concordaram, pelo menos em certa medida, que sua contribuição foi levada em consideração.

- Junto com pequenas organizações (26%), organizações sem fins lucrativos (67%) e organizações de telecomunicações (40%) também não sentiram que suas contribuições foram levadas em conta.

Q20. As contribuições são levadas em conta



ACHADOS

Intercâmbio de informações entre os setores público e privado

- Outra explicação possível para a falta de confiança ou crença na cooperação é a própria falta de cooperação formal. Cerca de 51% das organizações não pertenciam a nenhuma organização pública ou privada de compartilhamento de informações de segurança cibernética, com pouca variação entre setores ou tamanho de empresa.

- Através da cooperação contínua e do compartilhamento de informações, tanto no âmbito público/privado como privado/privado, as organizações podem aumentar suas capacidades de segurança cibernética e evitar a ocorrência de incidentes cibernéticos em larga escala. A cooperação deve ser inclusiva e multissetorial.

Recomendações

RECOMENDAÇÕES

Orçamento

Os governos devem trabalhar com organizações em seus países para identificar barreiras ao aumento dos orçamentos de segurança cibernética. Uma vez identificadas as barreiras, os governos podem desenvolver abordagens personalizadas para garantir que certas organizações que representam riscos para os cidadãos e a sociedade tenham assistência adequada para proteger adequadamente os dados e as redes. Se as pequenas organizações não tiverem orçamentos suficientes para fornecer programas robustos de segurança cibernética, os governos devem buscar bolsas de estudo e serviços compartilhados destinados a essas pequenas organizações. Elementos desses esforços governamentais devem incluir avaliação de risco, patches e exercicios de simulação.

Tipos de ataques

Os ataques de phishing podem ser um sintoma de uma categoria mais ampla de comprometimento de e-mails comerciais, bem como o modo inicial de entrega dos dois próximos que mais responderam aos ataques: ransomware e malware. Os governos devem explorar treinamentos e serviços compartilhados que possam ajudar as organizações a reduzir o risco de comprometimento de e-mails comerciais. Além disso, é fundamental que as organizações aprendam e aumentem sua resiliência aos ataques realistas da engenharia social. Portanto, os governos devem seguir políticas que exijam que as organizações aproveitem regularmente as atividades de red teaming. Esta abordagem de testes de segurança simula ataques que um ator ameaçador pode realizar, incluindo tentativas de influenciar funcionários para divulgar informações.

Eliminação de silos

O governo deve encorajar as organizações a desenvolverem uma estratégia baseada em soluções que elimine os silos de segurança cibernética e, em vez disso, contar com tecnologia que coordene/corrija as soluções de defesa existentes e lhes permita extrair valor adicional dessas ferramentas existentes.

Avaliação de risco

as evidências mostram um investimento extenso e inadequado na avaliação regular de riscos de segurança. Os governos devem explorar campanhas específicas para criar estruturas de segurança cibernética que exijam que as organizações realizem avaliações de riscos de segurança contínuas, incluindo revisões de código fonte em empresas de desenvolvimento de software, permitindo que elas identifiquem e solucionem os pontos fracos na preparação para o panorama de ameaças em evolução. Como as pequenas organizações podem ter menos visibilidade dos riscos, os governos devem buscar subsídios governamentais para permitir que essas organizações realizem tais avaliações.

Aplicação de patches

Os governos devem seguir políticas que exigem que as organizações de desenvolvimento de software façam um inventário dos componentes de seus produtos através de um software Bill of Materials (SBOM), alavancar a análise da composição do software (SCA) de forma contínua para identificar componentes vulneráveis e tomar medidas para comunicar e mitigar os riscos detectados. Os governos também devem considerar campanhas de educação direcionadas em todas as indústrias para implementar estruturas de segurança cibernética que exijam a aplicação de patches sempre que seja necessário. Além disso, os governos devem explorar se as organizações menores precisam ter acesso a serviços compartilhados ou recursos governamentais para aplicar os patches de forma eficaz e oportuna.

RECOMENDAÇÕES

Avaliação do engajamento

Os governos devem encorajar as organizações dos setores público e privado a trabalharem sistematicamente para identificar conexões com a infra-estrutura maliciosa conhecida de forma contínua e bloqueá-las imediatamente para reduzir as interrupções das operações comerciais e outras consequências negativas.

Operações de segurança cibernética

Faz-se necessário que as organizações mudem sua abordagem para resolver problemas de segurança cibernética de uma abordagem baseada exclusivamente em tecnologia para uma abordagem que combine operações de segurança cibernética mais tecnologia, aumentando a visibilidade e a capacidade de orquestração de sua atual pilha de segurança cibernética com mecanismos que forneçam feedback operacional e construam resiliência cibernética.

Segurança na nuvem

Muitos dos riscos descobertos no estudo podem ter ambientes em nuvem como superfície de ataque, onde surgem preocupações adicionais, tais como erros de configuração. Os governos devem implementar políticas que considerem esses riscos de segurança cibernética, mas que também permitam às organizações aproveitar os controles de segurança nativos e aumentados na nuvem para melhorar suas estratégias de segurança. O equilíbrio certo entre conformidade e verdadeira gestão de risco na nuvem pública enquanto se beneficia de uma infra-estrutura de nuvem fundamentalmente segura pode ser um bom facilitador para as estratégias de segurança.

Autenticação multi-fator

Os governos devem implementar políticas para encorajar/exigir que grandes organizações implementem a AMF ao acessar sistemas que processam informações sensíveis.

Frequência dos exercícios de simulação

Dada a constante ameaça de ataques cibernéticos, os governos devem implementar políticas que exijam que as organizações testem efetivamente seus planos de resposta a incidentes. Tal avaliação é possível com exercícios de red teaming. Estas referem-se a simulações de cenários do mundo real em que um grupo de analistas de segurança assume a responsabilidade de atacar a organização, enquanto a equipe de resposta da organização avalia o estado da segurança e organiza, implementa e melhora os controles de segurança.

Alta administração e diretoria

Os dados da pesquisa refletem uma confiança desigual nos conhecimentos dos executivos sobre C-suite. Os governos devem se concentrar em fornecer expectativas claras sobre o nível de conhecimento da alta administração e da diretoria em matéria de segurança cibernética.

Seguro de segurança cibernética

Os governos devem pesquisar as opções disponíveis para incentivar as organizações a obter um seguro que seja eficaz na redução do risco de segurança cibernética. Os governos devem considerar se há apólices de seguro disponíveis que sejam acessíveis e úteis na mitigação de riscos. As empresas podem utilizar soluções de avaliação do engajamento para demonstrar a maturidade da segurança cibernética e reduzir os custos das políticas de risco cibernético.

Aplicação da lei e CERTs

Há uma grande desconfiança em toda a região sobre o trabalho com as equipes nacionais de resposta a emergências informáticas e de aplicação da lei. Os CERTs nacionais e regionais devem desenvolver uma estratégia coletiva para lidar com essa falta de confiança. Um elemento específico de tal estratégia deve ser como os governos devem levar em conta a contribuição do setor privado no processo de desenvolvimento de políticas.

Compartilhamento de informações sobre ameaças e vulnerabilidades

Os governos devem identificar mecanismos para incentivar todas as organizações a participar de órgãos de compartilhamento de informações, tais como os Centros de Compartilhamento e Análise de Informações (ISACs) específicos do setor.

Relatório

LATAM CISO

2023

LATAM CISO

Duke UNIVERSITY