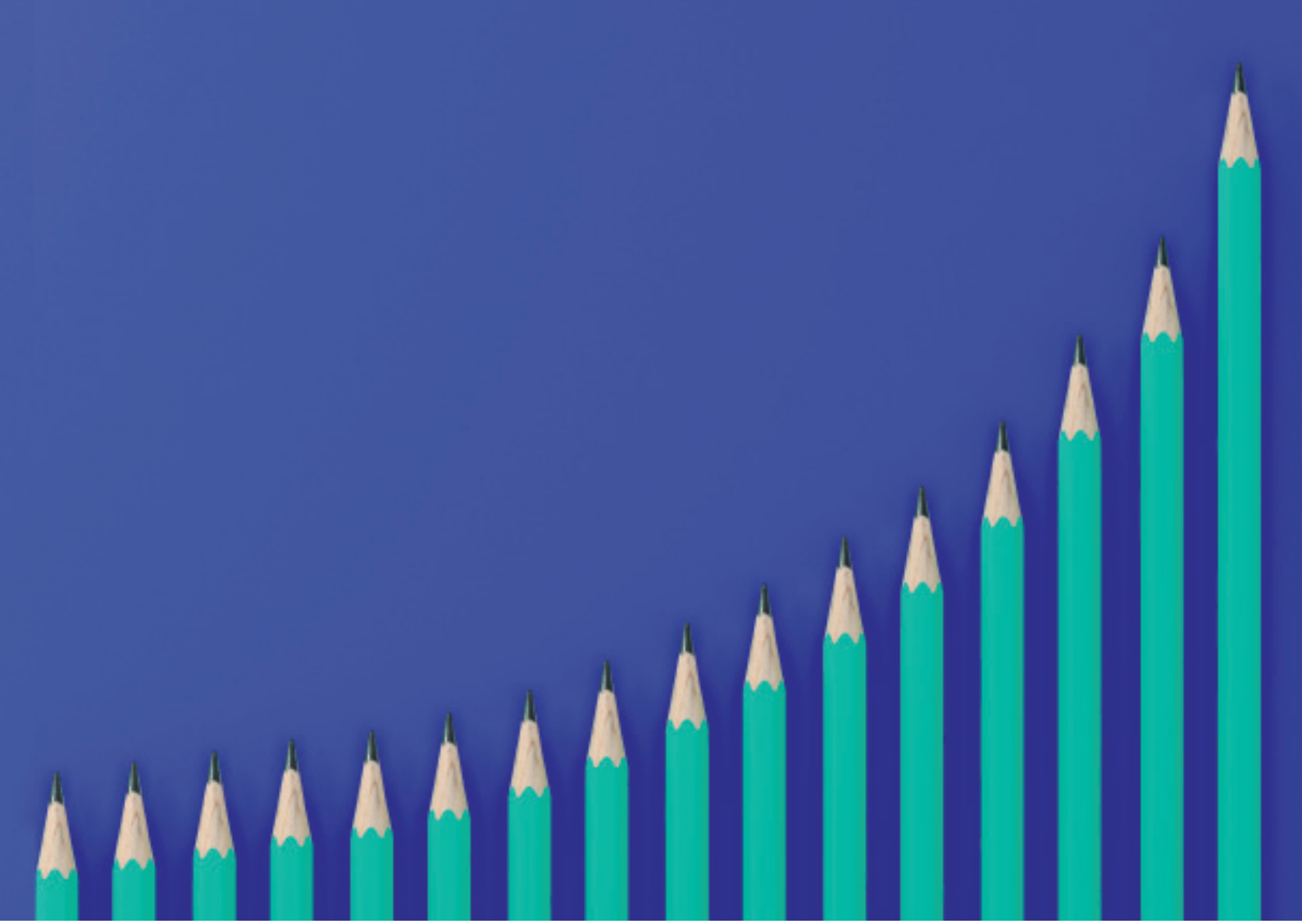


Como as empresas perdem dinheiro e economizam em meio aos ataques cibernéticos

Economia da segurança de TI em 2019

kaspersky BRING ON THE FUTURE

Contents

Metodologia

4,958 entrevistas

23 países

A Pesquisa de Riscos Globais de Segurança Corporativa de TI da Kaspersky (ITSRS) é uma pesquisa mundial com tomadores de decisões de TI nas empresas que está em sua 9ª edição anual. No total, foram realizadas 4.958 entrevistas em 23 países. Os participantes responderam a perguntas sobre o estado da segurança de TI em suas organizações, os tipos de ameaças que enfrentam e os custos incorridos ao recuperar-se de ataques. As regiões incluídas foram LATAM (América Latina), Europa, América do Norte, APAC (Pacífico Asiático com a China), Japão, Rússia e META (Oriente Médio, Turquia e África).

Ao longo de todo o relatório, as empresas são classificadas em PMEs (pequenas e médias empresas, com 50 a 999 funcionários) ou grandes corporações (empresas com mais de 1.000 funcionários). Nem todos os resultados da pesquisa estão incluídos neste relatório.

Todas as consequências financeiras e custos de ataques cibernéticos mencionados neste relatório estão relacionados apenas a incidentes que, segundo os participantes da pesquisa, levaram a violações de dados.

Introdução

É estimado que na primeira metade de 2019 terão aproximadamente 4,000 violações de dados, colocando mais de 4 bilhões de usuários em risco.

Enquanto os administradores de empresas se esforçam para preparar suas organizações para protegê-las de ameaças cibernéticas no futuro, a Kaspersky continua trabalhando para construir um mundo mais seguro. Isso envolve entender como as grandes corporações e as pequenas e médias empresas podem continuar identificando vulnerabilidades e se protegendo de ataques sofisticados.

Estima-se que, somente no primeiro semestre de 2019, houve quase 4.000 violações de dados que colocaram dados de mais de quatro bilhões de usuários em perigo. As organizações continuaram sendo afetadas por violações de cibersegurança importantes e custosas durante os últimos 12 meses. Neste ano, a Gartner informou que o investimento de orçamentos de infraestrutura e segurança de TI continuou aumentando. A projeção de gastos com TI no mundo inteiro é de US$ 3,74 trilhões em 2019, conforme as empresas devem reagir a um número crescente de ameaças a seus sistemas, operações de negócios e finanças.

Como essas empresas ainda se mostram vulneráveis a ataques cibernéticos, obviamente é preciso fazer mais para que elas possam se adaptar a um cenário de ameaças que muda rapidamente e cresce continuamente. Conforme se empenham nisso, observamos que as empresas continuam investindo em seus sistemas e na segurança de TI. O Financial Services Information Sharing and Analysis Center (FS-ISAC) recomenda que as empresas solicitem mais orçamento para cuidar da cibersegurança com agressividade, e isso deixa claro que as organizações precisam apoiar suas empresas para reduzir os riscos de longo prazo e se protegerem de ataques futuros previstos.

Complementando nossa pesquisa anual sobre a economia do setor de segurança de TI, este relatório reflete os resultados da pesquisa dos últimos 12 meses, destacando como as organizações estão investindo seu orçamento de segurança de TI. Ele examina como as empresas estão perdendo dinheiro e economizando frente aos ataques cibernéticos, e também como elas são afetadas pelo cenário de ameaças e as maneiras como estão reagindo a esses incidentes, tanto em termos financeiros quanto operacionais.

Principais resultados

Mais de um terço (38%) sentem que não tem conhecimento o suficiente das ameaças que seus negócios enfrentam

- Aumento da confiança: mais de metade (55%) das organizações está totalmente confiante de que sua rede não pode ser invadida, apesar de mais de um terço (38%) achar que não tem informações suficientes sobre as ameaças que suas empresas enfrentam

- As empresas estão negligenciando o perigo: apenas um décimo (12%) das grandes empresas se preocupam com infecções por malware, apesar desse ser o incidente de segurança mais custoso para elas, estimado em US$ 2,73 milhões

- O valor das pessoas: 66% das grandes corporações e PMEs desejam aumentar seus investimentos em equipes de especialistas neste ano

- Prevenidos, mas não preparados: as políticas que regulamentam o acesso de terceiros não estão reforçando a proteção das empresas, mas simplesmente triplicando o potencial de indenizações

- Aposte em seus pontos fortes: ter um Centro de operações de segurança interno reduz praticamente pela metade o impacto financeiro de violações de dados em grandes empresas, de US$ 1,4 milhão para apenas US$ 675 mil

- Os agentes de proteção de dados economizam seu dinheiro: mais de um terço (34%) das empresas que contam com um agente de proteção de dados não tiveram prejuízos financeiros ao sofrer violações de dados

Cada vez mais, negócios de todos os tamanhos se sentem mais confiante que sua rede está segura

As empresas precisam concentrar sua atenção nos ataques que custam mais caro

Apesar das empresas estarem aumentando seus orçamentos de segurança de TI e os recursos que investem no monitoramento de incidentes com ameaças, muitas não estão cientes dos ataques que custam mais dinheiro.

Cada vez mais, empresas de todos os tamanhos estão mais confiantes de que suas redes estão seguras. O número de empresas que declaram ter "100% de certeza de que suas redes não foram invadidas" é mais do que 10% maior que no relatório de 2016, com um aumento de 3% de um ano para outro. Porém, apesar dessa confiança, mais de um terço ainda acredita que não tem informações ou inteligência suficiente sobre os tipos de ameaças que suas empresas enfrentam.

Isso se reflete nos tipos de ameaças que afetam as empresas com as quais os pesquisados estão mais preocupados. Para empresas corporativas, as infecções por malware de dispositivos da empresa é a forma de violação de dados com maior impacto financeiro e custaram US $ 2,73 milhões neste ano, embora apenas uma pequena porcentagem das grandes empresas estar muito preocupada com a ameaça das infecções por malware.

As PMEs também estão ignorando as formas mais caras de ataques que sofrem. O tipo de violação de dados mais custoso para pequenas empresas são os incidentes que afetam infraestruturas de TI hospedadas por terceiros, que correspondem a US$ 162 mil. No entanto, as PMEs os classificaram apenas como o quinto mais importante e estão mais preocupadas com problemas que envolvem a proteção de dados, como a perda de um dispositivo físico ou a perda de dados devido a um ataque direcionado.

Investindo em pessoas e não em sistemas

O relatório do ano passado identificou que muitas empresas estavam embarcando em projetos de transformação digital para reestruturar seus sistemas e defendê-los de ataques cibernéticos, especialmente violações na nuvem. Contudo, os resultados deste ano mostram que, cada vez mais, as empresas estão investindo em pessoal e recursos para prevenir mais ataques e preparar seus departamentos de TI para o futuro.

Em 2019, as grandes corporações observaram o maior aumento de custos após incidentes decorrentes da utilização de profissionais externos (US$ 170 mil) e da contratação de funcionários novos (US$ 131mil), que aumentaram 35% e 24%, respectivamente, desde 2018. Nas PMEs, o custo de contratação de novas equipe continua o mesmo, em US$ 11 mil, quando comparado com outros gastos nos diferentes departamentos em geral. Além disso, as organizações enfrentam o desafio de poder investir em conhecimento para criar uma organização mais segura, pois não há talentos disponíveis para suprir a demanda do mercado.

Notadamente, isso resulta no fortalecimento das equipes internas de TI, em vez de simplesmente contratar MSPs terceirizados, levando as qualificações e o conhecimento para dentro da empresa.
O investimento em recursos dedicados e especialistas treinados internos também é uma forma de economia de longo prazo para as empresas após ataques de segurança. A pesquisa mostra que 34% de todas as empresas que têm um agente de proteção de dados (DPO) interno dedicado não tiveram prejuízos financeiros ao sofrer uma violação de dados. Nosso relatório deixa claro que esse investimento contínuo em pessoas e capacidade interna está se tornando fundamental para as empresas minimizarem as perdas financeiras e se protegerem de incidentes futuros.

Os Centros de operações de segurança estão se tornando cada vez mais importantes

Curiosamente, nosso estudo também mostrou que a maturidade dos sistemas de TI se reflete na economia obtida após violações de dados. Ter um Centro de operações de segurança interno reduz praticamente pela metade o impacto financeiro de violações de dados em grandes empresas, de US$ 1,4 milhão para apenas US$ 675 mil.

As PMEs maiores que adotam um SOC interno também economizam e, para elas, o impacto financeiro total de uma violação de dados é de apenas US$ 106 mil, em comparação com US$ 129 mil para as PMEs em geral. Embora essa economia não seja tão pronunciada, ainda assim ela reduz os custos em 22%, e ela pode ser menor, pois muitas PMEs ainda usam serviços externos para essa função.

Continue a leitura para saber mais detalhes sobre as conclusões do relatório.

Uso inadequado da TI resulta na forma mais frequente de violação de dados

Nosso relatório de 2019 mostrou que tanto as grandes corporações quanto as PMEs foram mais afetadas por incidentes decorrentes do uso inadequado dos recursos de TI pelos funcionários (52% nas grandes corporações, 50% nas PMEs), seguidos da infecção por malware de dispositivos de propriedade da empresa (51%, nas grandes corporações; 49% nas PMEs). Ou seja, as empresas deveriam tentar reduzir o risco de violações de dados reforçando o treinamento em segurança de dados dos funcionários para aumentar a conscientização sobre o uso seguro da TI.

Incidentes mais frequentes direcionados a PMEs

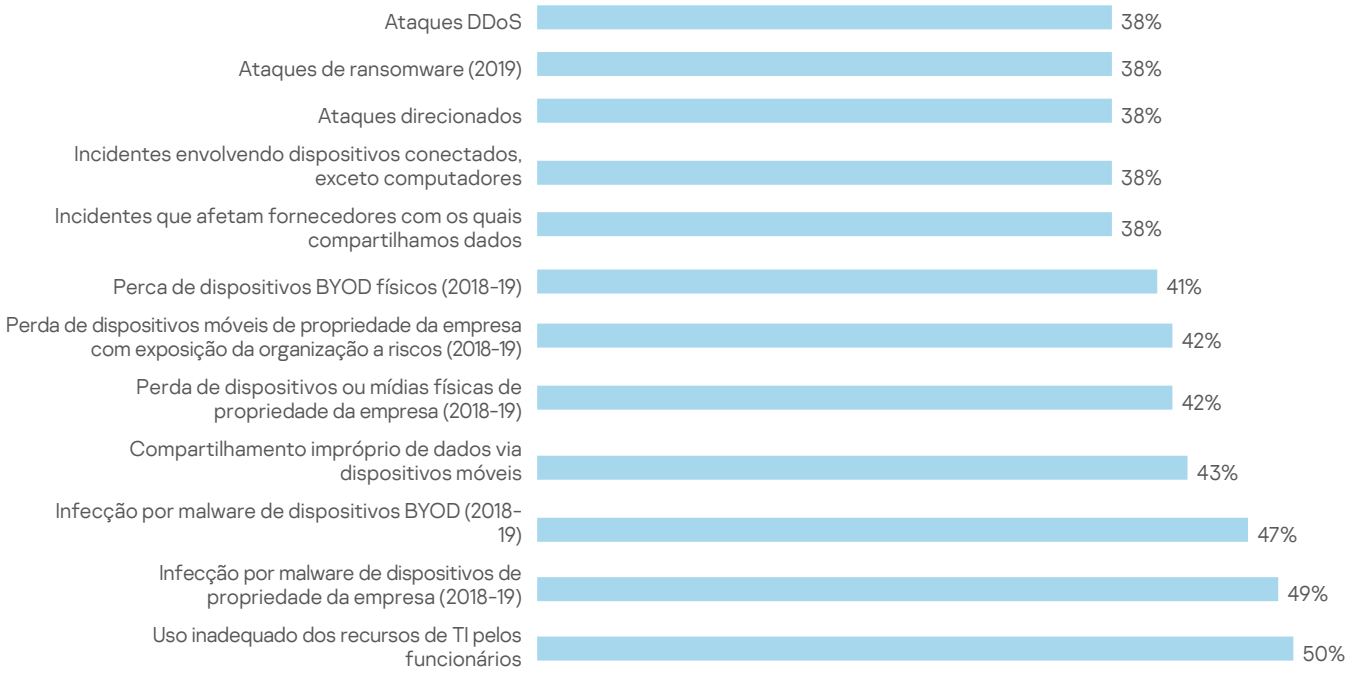


Figura 1. Incidentes mais frequentes direcionados a PMEs

Incidentes mais frequentes direcionados a grandes corporações

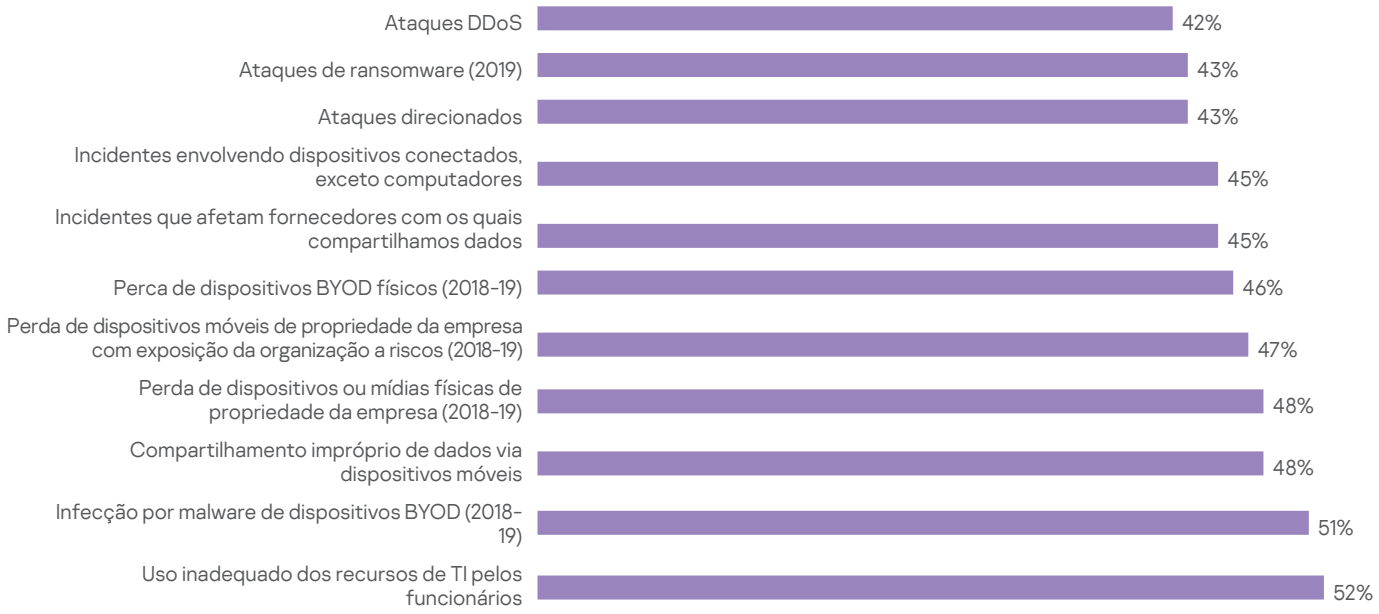


Figura 2. Incidentes mais frequentes direcionados a grandes corporações

Surpreendentemente, em 2019, as violações de dados mais custosas para as PMEs não foram, na verdade, as formas mais frequentes de incidentes de segurança. Neste ano, os três ataques mais custosos a PMEs foram incidentes que afetaram a infraestrutura de TI hospedada por terceiros (US$ 162 mil), ataques DDoS (US$ 138 mil) e ataques direcionados (US$ 138 mil). No entanto, em termos de frequência (veja a Figura 1.), eles ficam apenas em 16°, 12° e 10° lugar, respectivamente,
na segurança que mais visam PMEs.

Impacto financeiro médio de violação de dados por tipo em PMEs

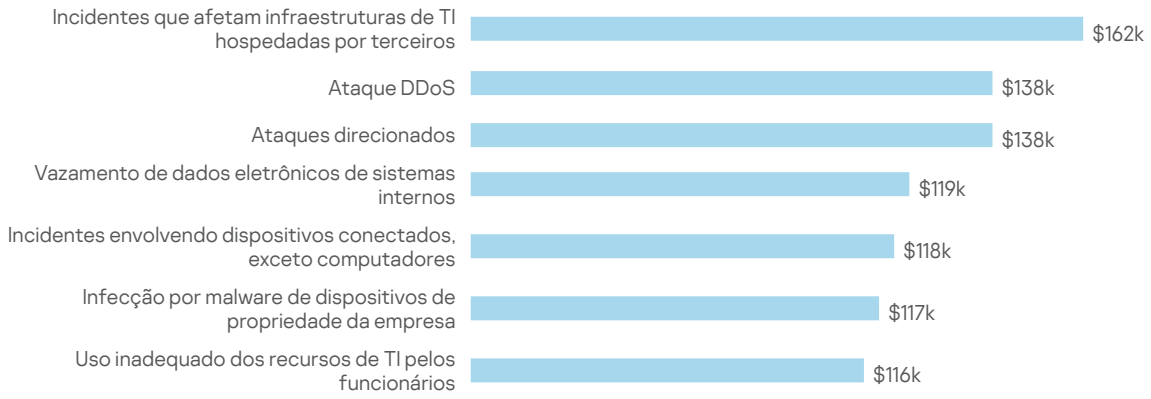


Figura 3. Impacto financeiro médio de violação de dados por tipo em PMEs

Os dados das grandes corporações são diferentes neste caso, onde as três violações de dados corporativas mais caras correspondem aos ataques mais frequentes: infecção por malware de dispositivos de propriedade da empresa (US$ 2,73 milhões), incidentes que afetam fornecedores com quem a empresa compartilhou dados (US$ 2,57 milhões) e perda física de dispositivos móveis de propriedade da empresa (US$ 1,69 milhões) aparecem dentre os seis primeiros na lista de incidentes de segurança mais frequentes. O incidente de segurança mais custos para as grandes empresas em 2019 foi a infecção por malware de dispositivos de propriedade da empresa. Notadamente, os ataques direcionados são apenas o quinto mais caro.

Impacto financeiro médio de violações de dados por tipo em grandes corporações

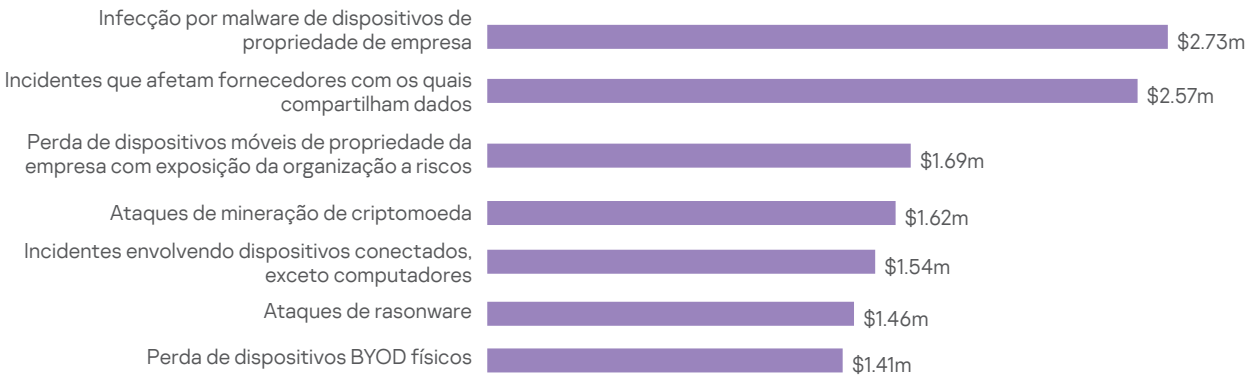


Figura 4. Impacto financeiro médio de violação de dados por tipo em grandes corporações

No entanto, quando se trata de incidentes que preocupam as empresas, as grandes corporações estão mais preocupadas com a perda de dados em consequência de um ataque direcionado (23%) do que com vírus e malware (13%). De maneira semelhante, os ataques direcionados são a maior preocupação das PMEs (23%) e a terceira forma de violação de dados mais custosa para as PMEs, correspondendo a US$ 138 mil.

Neste ano, 47% das PMEs e 51% das grandes corporações concordaram que está se tornando mais difícil diferenciar os ataques de segurança genéricos dos direcionados. Assim, é mais complicado para elas detectarem um incidente no meio do ruído ou avaliar o perigo potencial do incidente. Possivelmente, esse é um dos motivos por que estão se tornando suscetíveis a níveis cada vez maiores de ameaças de malware moderadas e avançadas.

No geral, o custo das violações de dados em grandes empresas aumentou, e o impacto financeiro de uma violação de dados média alcança US$ 1,41 milhão, tendo sido US$ 1,23 milhão no ano anterior. As maiores elevações de custos procedem do aumento da contratação de especialistas externos para corrigir a violação (US$ 170 mil) e do custo total dos negócios perdidos (US$ 163mil). A esse custo, soma-se a necessidade de pessoal extra de relações públicas para reparar os danos à marca após uma violação (US$ 161 mil).

Comparativamente, as PMEs tiveram um custo total de violações de dados de US$ 108 mil, abaixo dos US$ 120 mil de 2018 , com um valor menor gasto em indenizações (US$ 5 mil), negócios perdidos (US$ 13 mil) e software e infraestrutura (US$ 13 mil).

1 A redução do custo das violações de dados em PMEs também pode ter sido afetada pela alteração da amostra da pesquisa em 2019. A alteração da estrutura das amostras em algumas verticais podem introduzir necessidades específicas dos verticais.

As empresas pagam por pessoal, gestão de relações públicas e oportunidades de negócios perdidas

Quando uma empresa sofre um ataque de segurança, seja ela uma grande corporação ou uma PME, o aumento dos custos corporativos vem de diversas áreas, incluindo penalidades e multas, prêmios de seguros mais altos, novos softwares e treinamento. No entanto, segundo nossa pesquisa, especialistas externos e os recursos humanos foram os principais motivadores do aumento dos custos corporativos resultantes de um ataque cibernético em 2019.

Análise do impacto financeiro médio de uma violação de dados em grandes corporações

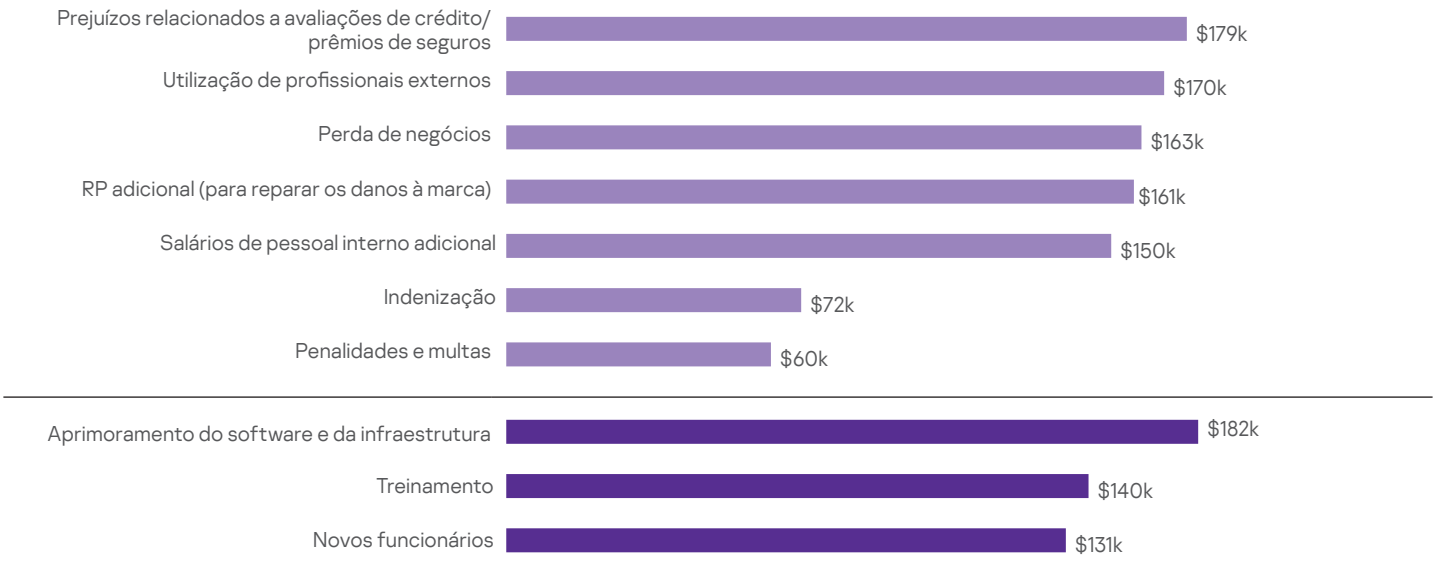


Figura 5. Análise do impacto financeiro médio de uma violação de dados em grandes corporações

Análise do impacto financeiro médio de uma violação de dados em PMEs

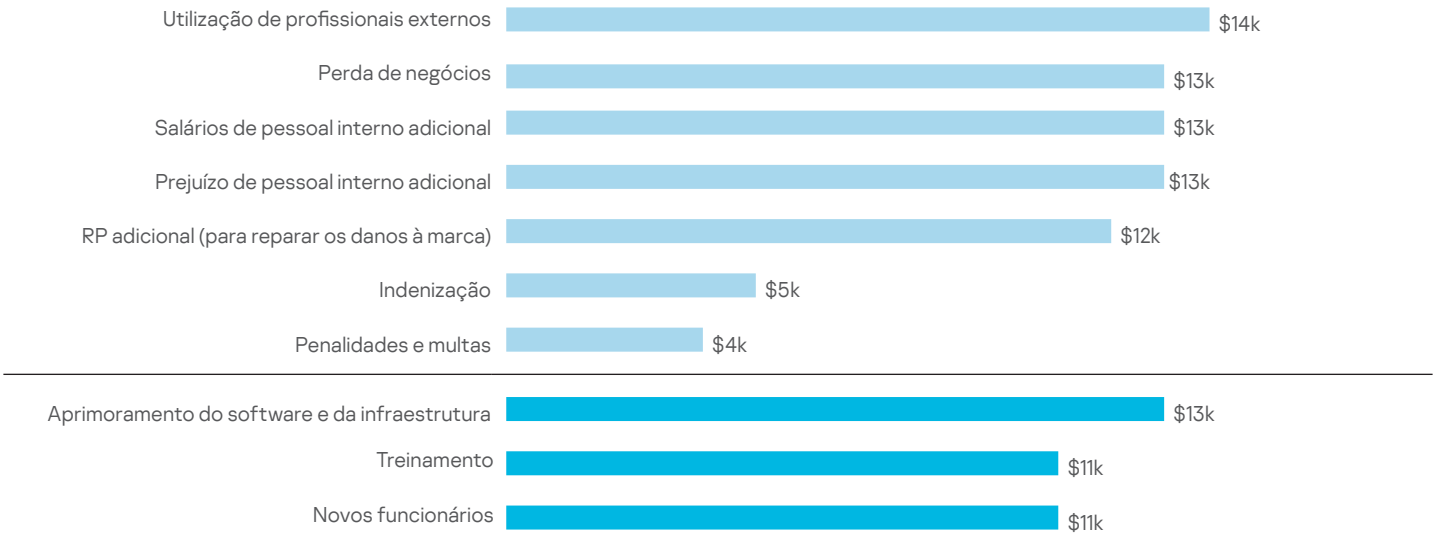


Figura 6. Análise do impacto financeiro médio de uma violação de dados em PMEs

Nas grandes corporações, o aumento de custos de um ano para outro mais significativo deve-se à utilização de profissionais externos (US$ 170 mil) e à contratação de novos funcionários (US$ 131 mil), que aumentaram 35% e 24%, respectivamente, desde 2018.

Impacto financeiro médio de uma violação de dados em grandes empresas

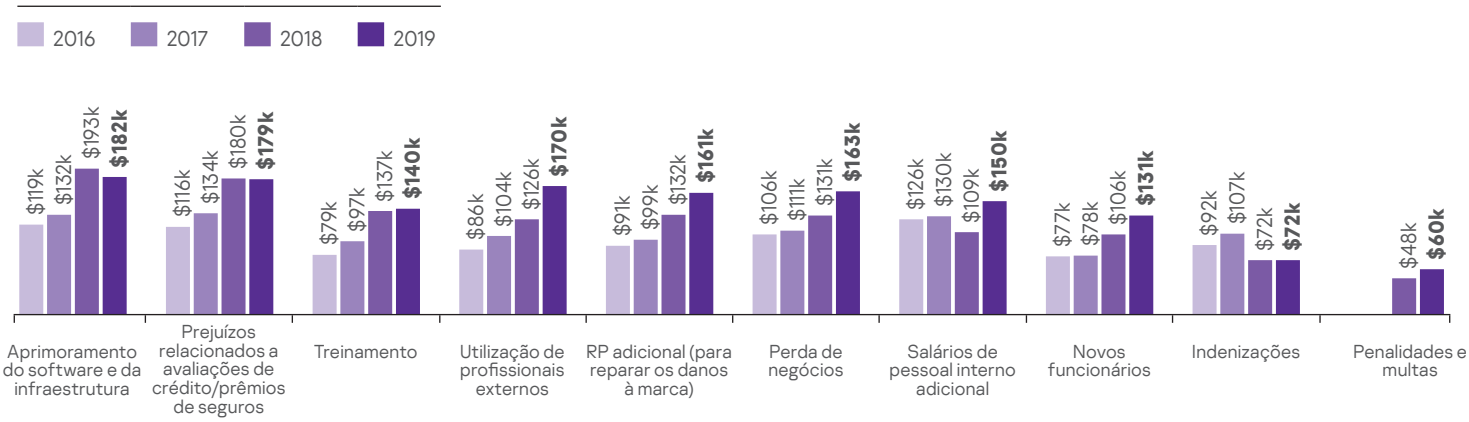


Figura 7. Impacto financeiro médio de uma violação de dados em grandes corporações

Ao mesmo tempo, os níveis gerais de despesas das PMEs relacionadas a ameaças estão diminuindo. Porém, os gastos com novos funcionários continuam inalterados, em US$ 11 mil, o que mostra que as PMEs continuam investindo na especialização da equipe para estar mais preparadas para problemas de segurança.

Impacto financeiro médio de uma violação de dados em PMEs

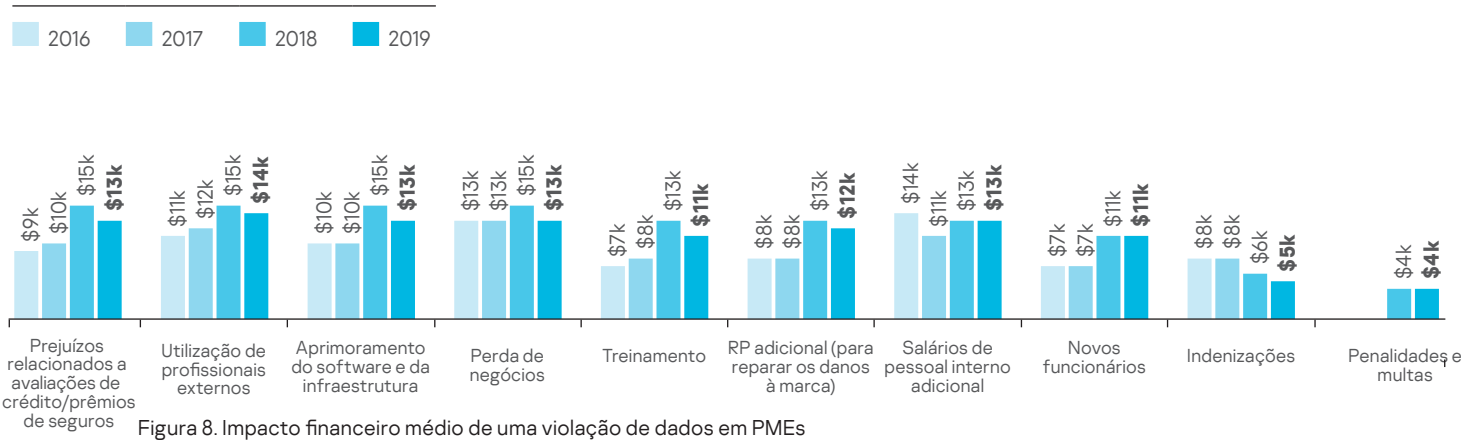


Figura 8. Impacto financeiro médio de uma violação de dados em PMEs

A perda de negócios novos ou existentes também gera um custo importante para todos os tipos de empresas que sofrem um incidente. Neste ano, as infecções por malware ficaram no alto da lista de violações mais custosas para as grandes corporações, enquanto as PMEs foram mais afetadas financeiramente pelos ataques direcionados. Nos dois casos, os maiores custos para cada setor vieram da perda de negócios decorrente dos ataques, representando US$ 331 mil de receita perdido para as grandes corporações afetadas por uma infecção por malware e US$ 22 mil para as PMEs que sofreram um ataque direcionado.

Relações públicas em caso de escândalos e incidentes com ameaças: Conforme escândalos de violações de dados corporativos aparecem com mais frequência nas notícias, o público sabe cada vez mais sobre os incidentes que envolvem a segurança de seus dados. Isso pode gerar uma falta de segurança e confiança do público nas empresas, e elas precisam investir em relações públicas e gestão de crises para restaurar a confiança dos clientes em sua marca. Nossa pesquisa mostrou que 31% das PMEs e 36% das grandes corporações tiveram problemas de relações públicas em 2019 por conta de violações de dados com consequente impacto financeiro adicional.

Cada vez mais, as empresas estão utilizando políticas de acesso de terceiros, usando-as para reduzir os riscos de incidentes de segurança. Mas será que essas políticas realmente reduzem a probabilidade de violações de dados? Segundo nossa pesquisa, 79% das grandes corporações e 75% das PMEs implementaram políticas especiais para regulamentar o acesso de fornecedores aos dados corporativos.

Outras partes estão sujeitas a políticas de segurança de TI?

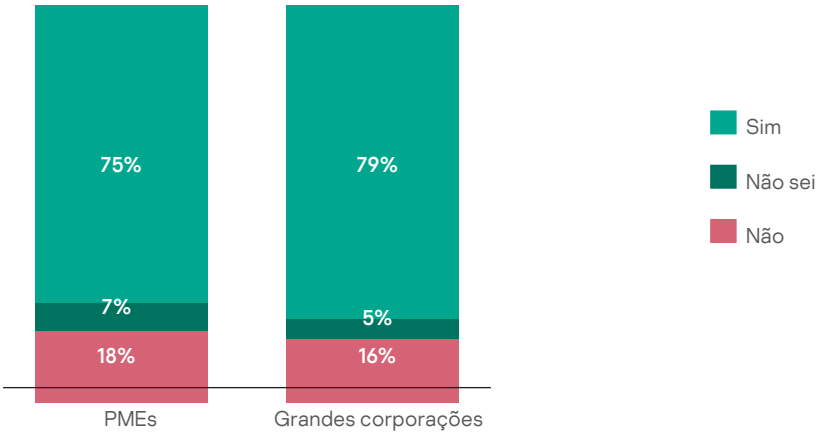


Figura 9. Outras partes estão sujeitas a políticas de segurança de TI?

Políticas de acesso de terceiros e violações de dados em PMEs

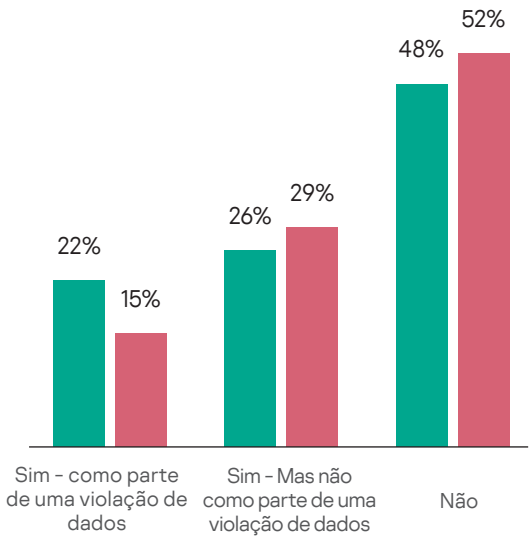


Figura 10. Políticas de acesso de terceiros e violações de dados em PMEs

Políticas de acesso de terceiros e violações de dados em grandes corporações

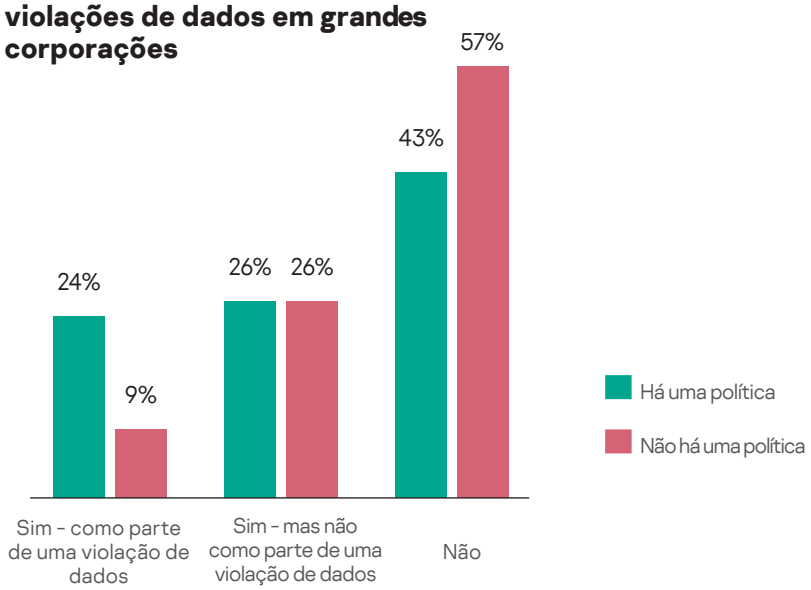


Figura 11. Políticas de acesso de terceiros e violações de dados em grandes corporações

Como mostram as Figuras 10 e 11, é claro que essas políticas não tornaram esses incidentes menos frequentes, mas aumentaram muito a probabilidade de uma empresa receber indenizações após uma violação de dados envolvendo terceiros. Como mostra a Figura 12 abaixo, 71% das grandes corporações com uma política para terceiros registrada receberam indenizações em 2019, em comparação com apenas 22% das empresas que não tinham uma política em vigor.

Políticas de acesso de terceiros e indenização em grandes corporações

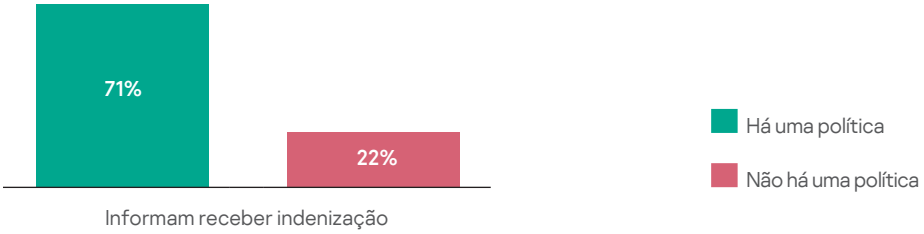
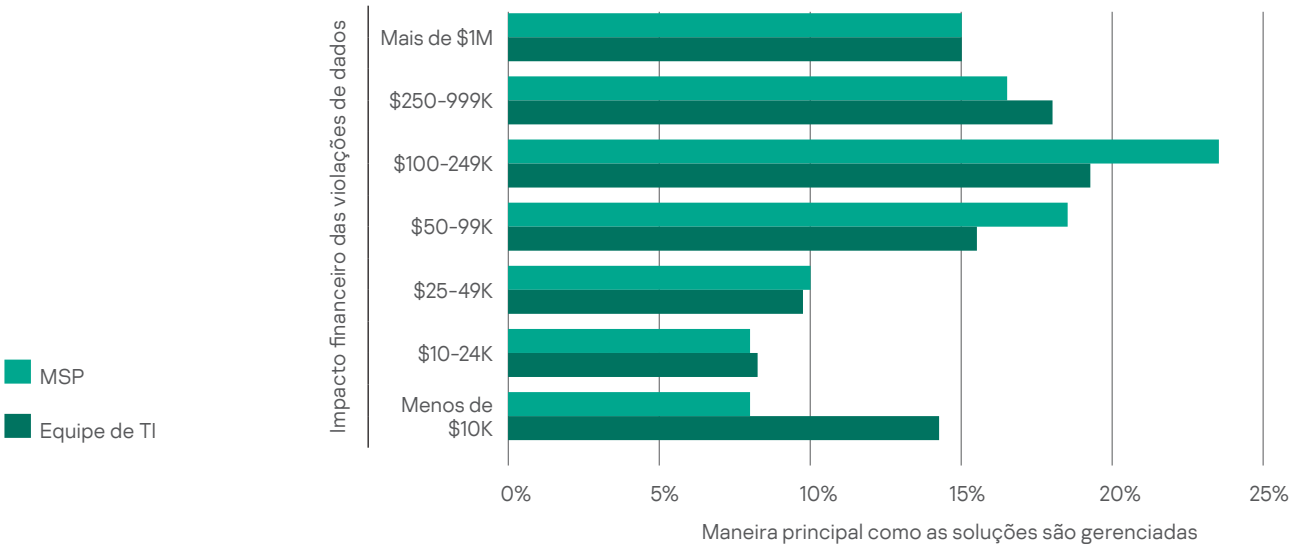


Figura 12. Políticas de acesso de terceiros e indenização em grandes

Ao deparar-se com os crescentes custos de segurança de TI, muitas organizações acham que a terceirização de suas equipes de TI pode gerar economias. Porém, provedores de serviços de cibersegurança descuidados ou pouco qualificados podem sair mais caro para a empresa em caso de um incidente. De todas as empresas que sofreram uma violação de dados com impacto financeiro entre US$ 100 – 249 mil, 23% tinham a segurança terceirizada para um MSP, enquanto apenas 19% tinham equipes de TI internas.

Impacto financeiro total de violação de dados: Terceirização VS gerenciamento interno de segurança de TI



A maturidade leva à economia: empresas com DPOs e SOCs minimizam os custos de uma violação

Organizações com um agente de proteção de dados (DPO) têm menos probabilidade de sofrer prejuízos financeiros. 34% das empresas que têm um DPO não perderam receita após um ataque, em comparação com 20% das empresas que não têm esse cargo. Mas, claro, embora isso possa reduzir as perdas, ter o cargo dedicado não garantirá a proteção contra violações de dados.

Para as grandes corporações, ter um centro de operações de segurança pode reduzir significativamente os custos de violações de dados. Em 2019, eles foram de apenas US$ 675 mil para empresas com SOCs, em comparação com uma média de US$ 1,41 milhão para as empresas em geral.

No entanto, simplesmente denominar a equipe de segurança de sua empresa de SOC não tem o mesmo efeito: nossa pesquisa mostrou que, se um SOC realiza funções gerais de segurança de TI, ele não afeta o impacto financeiro de uma violação de dados. É necessário ter treinamento, especialização e sistemas dedicados para que haja essa redução dos custos após uma violação.

Como os orçamentos direcionados à segurança de TI estão mudando?

Segundo a Gartner, as despesas gerais das empresas com segurança estão aumentando. Isso é confirmado pela pesquisa deste ano, em que as despesas das PMEs alcançaram US$ 267 mil, em comparação com US$ 256 mil em 2018. Esse crescimento é ainda mais pronunciado nas grandes corporações, cujos orçamentos de segurança aumentaram mais do que duas vezes, chegando a US$ 18,9 milhões, em relação aos US$ 8,9 milhões do último ano. Espera-se que esse valor aumente mais 11% ao longo dos próximos três anos.

Proporção do orçamento de TI das empresas alocada para a segurança de TI

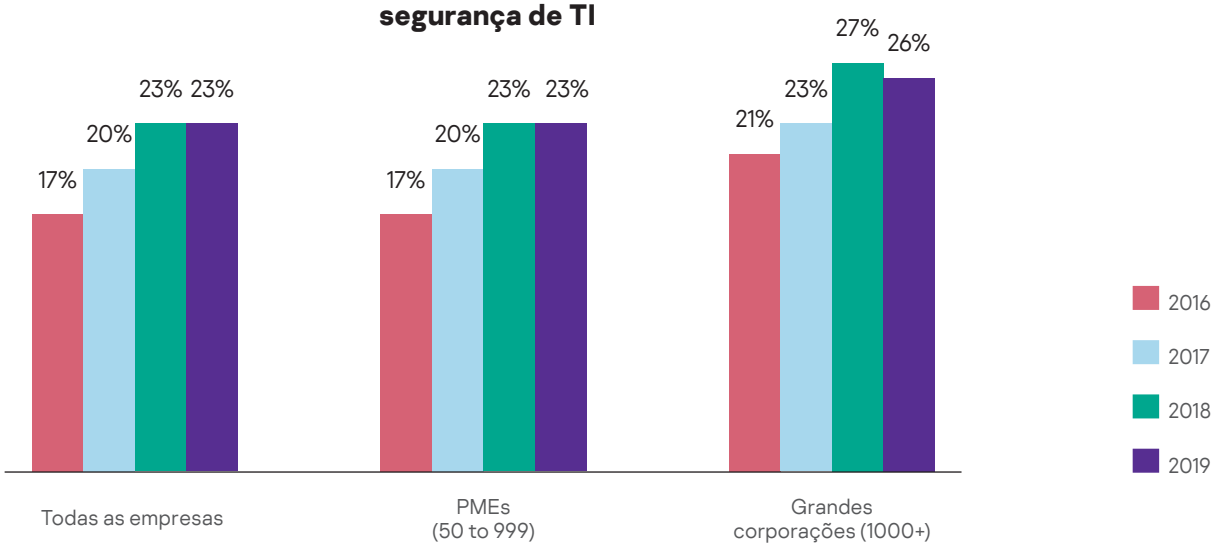


Figura 14. Proporção do orçamento de TI das empresas alocada para a segurança de TI

Apesar do aumento, os orçamentos direcionados à segurança de TI não estão absorvendo uma porcentagem maior dos orçamentos gerais de TI das empresas. Neste ano, a proporção geral da segurança de TI em termos percentuais dos gastos gerais com TI permaneceu igual nas PMEs, com 23% em 2018 e 2019, e até diminuiu um pouco nas grandes corporações, com uma parcela de 27% do orçamento total em 2018 e 26% em 2019.

Isso poderia ser explicado pelos grandes investimentos feitos em anos anteriores. Muitas grandes violações de dados, como a violação do banco de dados de cartões de crédito da Capital One, que divulgou dados de 106 milhões de clientes, ou o incidente com o Facebook, em que centenas de milhões de registros de usuários foram expostos em um servidor de nuvem da Amazon, o lançamento da GDPR e as transformações digitais generalizadas catalisaram grandes investimentos na cibersegurança corporativa ao longo dos últimos anos. Agora, parece que as empresas atingiram um limite relativamente estável, de aproximadamente 25%, e podem estar começando a reavaliar o lucro gerado por esses investimentos anteriores antes de aprimorar sua cibersegurança.

Onde as PMEs e grandes corporações estão investindo seu orçamento de TI

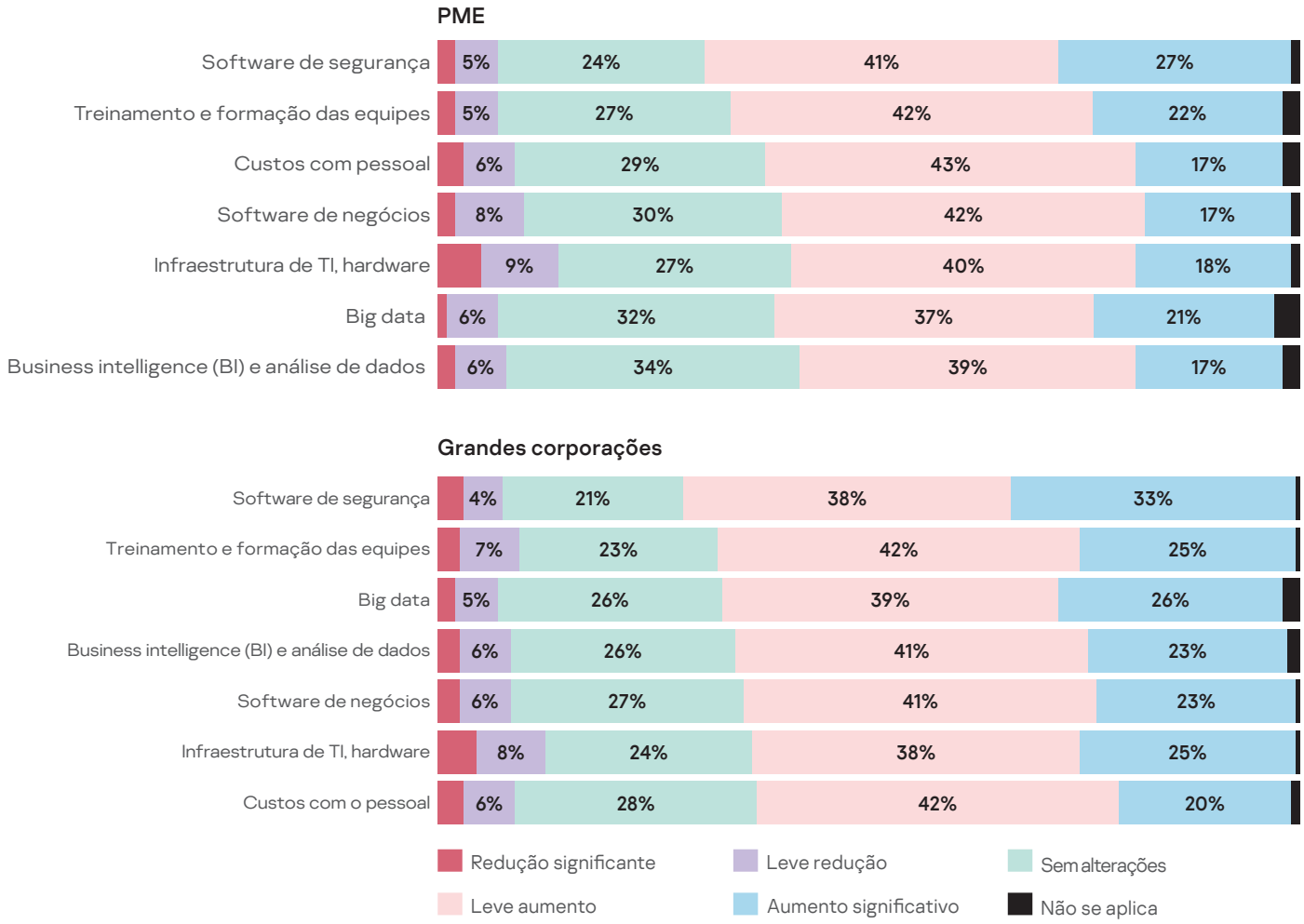


Figura 15. Onde as PMEs e grandes corporações estão investindo seu orçamento de TI

Quando se trata de investir no futuro, as empresas estão usando seus orçamentos de TI principalmente para aumentar seus investimentos em software de cibersegurança, treinamento e formação das equipes. Como mostra a Figura 15 acima, 33% das grandes corporações e 27% das PMEs tiveram um aumento significativo das despesas com software de segurança. Tanto as grandes corporações quanto as PMEs também fizeram investimentos significativos em programas de Big Data (26% nas grandes corporações, 21% nas PMEs) e no treinamento e formação de equipes (25% nas grandes corporações, 22% nas PMEs).

A adesão dos altos executivos leva ao aumento nos orçamentos de cibersegurança

Em empresas nas quais os altos executivos estão muito envolvidos no processo de decisões de TI, o orçamento médio de segurança de TI chega a mais de US$ 5 milhões, tanto nas grandes corporações quanto nas PMEs. Em comparação, o orçamento médio em empresas nas quais a direção executiva está apenas parcialmente envolvida é de US$ 10 - 12 mil.

Despesas com a segurança de TI e envolvimento dos altos executivos

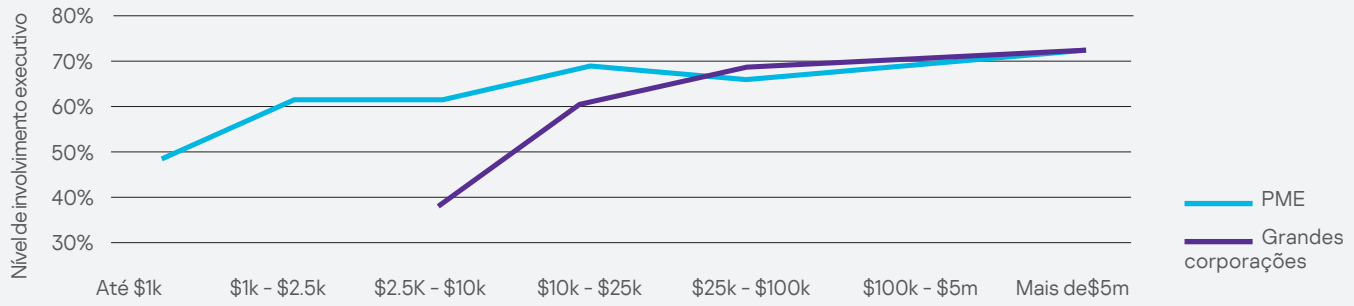


Figura 16. Despesas com a segurança de TI e envolvimento dos altos executivos

Conclusão

É vital que os negócios continuem investindo e repensando seus processos segurança de TI de maneira a estarem um passo a frente das taxas de crescimento de cyber ataques, e limitar quaisquer perdas financeiras incorridas.

Nosso relatório destaca que, quando uma empresa investe em pessoal, recursos e processos, ela é capaz de lidar melhor com os resultados e os prejuízos financeiros dos incidentes de cibersegurança.

Empresas que têm um DPO especializado, que criaram um SOC interno ou introduziram regulamentações para terceiros que têm acesso aos dados da empresa observaram uma redução nos prejuízos financeiros ou tiveram a capacidade de resgatar alguns custos após uma violação de dados.

Cada vez mais, os líderes de negócios também estão se envolvendo no processo de tomada de decisões relacionadas à segurança de TI. Isso resulta em orçamentos maiores para a segurança de TI e na melhor preparação para a gestão de incidentes. Assim, tanto para as PMEs quanto para as grandes corporações que desejam investir mais em suas atividades de cibersegurança, é fundamental obter o interesse dos altos executivos.

No entanto, nem todas as empresas estão preparadas como poderiam para a ameaça de um ataque. A percepção geral entre as empresas é de que o número de ameaças a suas redes está diminuindo, apesar dos incidentes de todos os tipos continuarem aumentando em 2019. Considerando que apenas um décimo (12%das grandes corporações preocupa-se com infecções por malware, mesmo sendo esse o incidente de segurança mais custoso, é claro que as empresas precisam estar mais conscientes de quanto esses ataques custam às empresas, independentemente de sua frequência.

De maneira semelhante, a porcentagem do orçamento dedicado à segurança de TI permaneceu igual em comparação com o ano anterior, possivelmente mostrando que os investimentos em segurança de TI começaram a empacar enquanto as empresas consideram como vão abordar a questão no futuro. Dado o risco contínuo de ataques, em vez de esperar, as grandes corporações e PMEs devem continuar investindo no futuro para estarem preparadas para a próxima geração de incidentes de segurança. É fundamental que as empresas continuem investindo e repensando seus processos de segurança de TI para que estejam um passo à frente dos crescentes índices de ataques cibernéticos, e para limitar os prejuízos financeiros sofridos.

É claro que muitas empresas enfrentam desafios para conseguir os especialistas certos para se protegerem de ameaças de cibersegurança. Por isso, para garantir a segurança, é essencial priorizar e investir em conhecimento de cibersegurança, interna ou externamente, por meio de um fornecedor.

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com/

kaspersky BRING ON THE FUTURE

perdas financeiras incorridas.