VELHOS HÁBITOS NUNCA MORREM:

Como os desafios relacionados a pessoas, processos e tecnologias prejudicam as equipes de segurança cibernética no Brasil

UMA PUBLICAÇÃO DA TENABLE BASEADA EM UM ESTUDO ENCOMENDADO COM 825 PROFISSIONAIS DE TI E SEGURANÇA CIBERNÉTICA, INCLUINDO 50 ENTREVISTADOS BRASILEIROS, CONDUZIDO PELA FORRESTER CONSULTING EM 2023

FORRESTER®

Índice

Publicação/Velhos hábitos nunca morrem/02/11/23

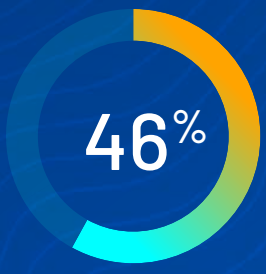
Introdução

Quando falamos em reduzir o risco cibernético, organizações do mundo todo se veem limitadas por questões relacionadas a pessoas, processos e tecnologias. Juntos, esses desafios dificultam muito a prática eficaz de segurança cibernética preventiva pelas organizações, mesmo com o aumento da complexidade da superfície de ataque. Quando falamos em aplicação proativa de patches a vulnerabilidades de software, muitas organizações ainda enfrentam dificuldades com o básico. Abordar preventivamente as configurações incorretas do sistema também continua sendo um desafio. Para complicar ainda mais as coisas, as organizações têm o desafio de obter uma imagem precisa da sua superfície de ataque, incluindo visibilidade de ativos desconhecidos, recursos de nuvem, pontos fracos de código e sistemas de direitos dos usuários.

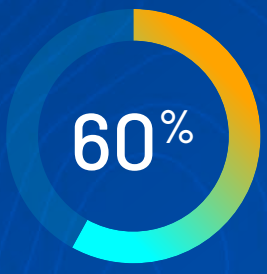
Qualquer área de exposição acima representa várias vias possíveis que um invasor pode explorar para comprometer a organização. Por meio de um estudo encomendado com 825 líderes de TI e segurança cibernética, incluindo 50 entrevistados brasileiros, conduzido pela Forrester Consulting em nome da Tenable em 2023, pretendemos entender como os seguintes desafios relacionados a pessoas, processos e tecnologias enfrentados pelas equipes modernas de TI e segurança cibernética prejudicam práticas eficazes de redução de riscos:

DESAFIOS RELACIONADOS A PESSOAS

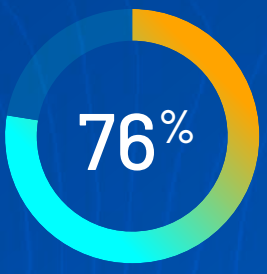
As equipes de TI e segurança cibernética costumam ficar isoladas, e o desempenho delas é avaliado por meio de metas e critérios distintos e contraditórios. As atitudes internas fazem com que a coordenação entre as equipes de TI e segurança seja difícil e demorada.



Quase metade (46%) considera a coordenação entre as equipes de TI e segurança cibernética difícil e demorada.



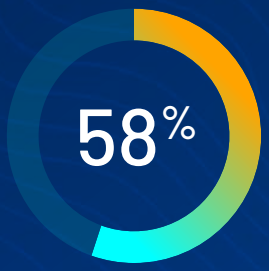
Seis em cada 10 (60%) afirmam que a equipe de segurança cibernética fica ocupada demais com incidentes críticos para adotar uma abordagem preventiva a fim de reduzir a exposição da organização.



Quase oito em cada 10 (76%) afirmam que a TI está mais preocupada com o tempo de atividade do que com a aplicação de patches/correções.

DESAFIOS RELACIONADOS A PESSOAS (CONTINUAÇÃO)

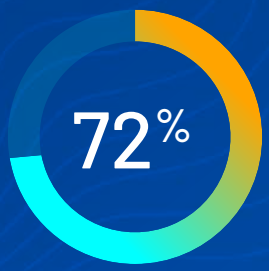
São necessários recursos humanos consideráveis para gerenciar as diversas ferramentas usadas para praticar a segurança cibernética preventiva e gerar relatórios de risco significativos com base nessas fontes de dados discrepantes.



Seis em cada 10 entrevistados (58%) têm 25 ou mais funcionários dedicados à implementação, ao suporte, à manutenção e/ou ao relacionamento com fornecedores das ferramentas de segurança cibernética preventiva que utilizam.

Em média, as organizações gastam 14 horas por mês gerando relatórios de segurança para líderes corporativos.

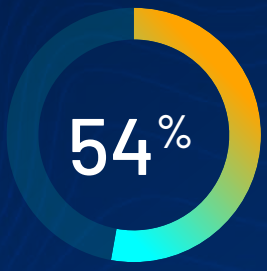
Nos últimos dois anos, descobrimos que uma organização média estava preparada para defender preventivamente 59% dos ataques cibernéticos sofridos. Porém, esse nível de cobertura as deixa vulneráveis a 41% dos ataques. As empresas foram forçadas a mitigá-los de forma reativa, em vez de impedi-los de uma vez.



Quase três quartos (72%) acreditam que a organização teria mais sucesso na defesa contra ataques cibernéticos se dedicasse mais recursos à segurança cibernética preventiva.

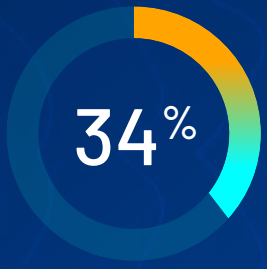
DESAFIOS RELACIONADOS A PROCESSOS

Os invasores avaliam os ambientes o tempo todo. Porém, na maioria das organizações, reuniões sobre sistemas críticos para o negócio são realizadas com frequência mensal (na melhor das hipóteses!).

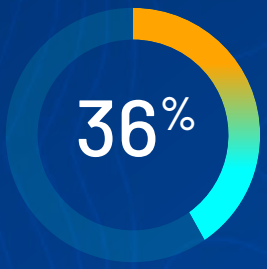


Na maior parte das organizações (54%), os líderes de TI e segurança reúnem-se mensalmente com os líderes corporativos para discutir os sistemas críticos para o negócio. Em mais de 26% das organizações, essas reuniões acontecem apenas uma vez por ano (ou menos). Como os invasores avaliam o ambiente de forma contínua, acreditamos que comunicações e reuniões mais frequentes para tratar a criticidade dos sistemas para o negócio são essenciais para reduzir os riscos.

Quando há interesses concorrentes, muitas vezes a segurança cibernética não é consultada com antecedência suficiente (quando isso sequer ocorre) na implementação de serviços em nuvem.

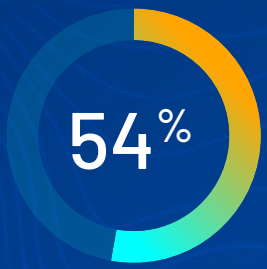


Mais de um terço dos entrevistados (34%) afirma que a equipe de segurança cibernética não é consultada com antecedência suficiente no processo de escolha e implementação de serviços em nuvem.



Além disso, 36% afirmam que suas equipes de negócio e engenharia compram e implementam serviços em nuvem sem informar a equipe de segurança cibernética.

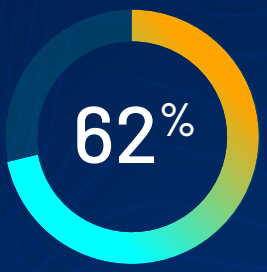
Problemas de higiene de dados atrapalham uma priorização eficaz.



Quase seis em cada 10 entrevistados (54%) afirmam que a falta de higiene dos dados os impede de obter dados de qualidade dos sistemas de gestão de acesso e privilégios de usuários e dos sistemas de gerenciamento de vulnerabilidades. A segurança cibernética preventiva exige a habilidade de avaliar vulnerabilidades em contexto com os dados dos usuários, de modo que os funcionários de TI e segurança cibernética possam tomar decisões corretas de priorização referentes aos sistemas ou às classes de usuários e ativos que devem receber correção prioritária.

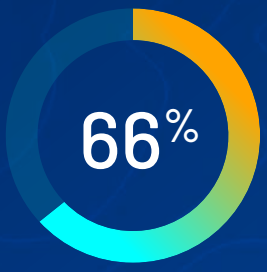
DESAFIOS RELACIONADOS A TECNOLOGIAS

Uma miscelânea de ferramentas de segurança cibernética preventiva faz com que seja desafiador para os líderes de TI e segurança cibernética obterem perspectivas significativas sobre a profundidade e a amplitude da exposição.

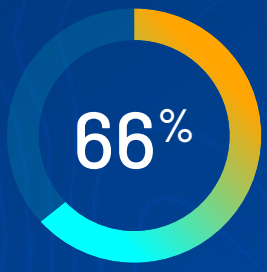


Seis em cada 10 entrevistados (62%) usaram dez ou mais ferramentas de segurança cibernética preventiva nos últimos 12–24 meses.

Profissionais que usam ferramentas isoladas não conseguem determinar a relação entre usuários, sistemas e software. Além disso, diferentes métricas de medição entre as diferentes ferramentas dificultam a avaliação precisa dos riscos.

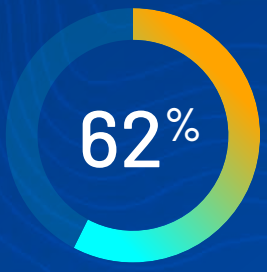


Embora a maioria dos entrevistados (66%) afirme levar em conta a identidade dos usuários e os privilégios de acesso ao priorizar a correção de vulnerabilidades, mais da metade afirma que a organização não tem uma maneira eficaz de integrar esses dados em suas práticas de segurança cibernética preventiva e gerenciamento de exposição.



Quase sete em cada 10 (66%) afirmam que seus sistemas isolados constituem uma barreira para a obtenção de dados dos usuários.

Três em cada cinco ferramentas de segurança cibernética utilizadas com frequência são reativas e não preventivas, dificultando a execução de práticas de segurança cibernética proativas.



Mais de seis em cada 10 organizações (62%) usaram 10 ou mais ferramentas de segurança cibernética preventiva nos últimos dois anos.

O que dificulta tanto a segurança cibernética preventiva?

Os órgãos governamentais e a comunidade de investidores nunca estiveram tão atentos aos programas de segurança cibernética como hoje. Com isso, muitas organizações sentem-se desafiadas no momento de relatar e comunicar os riscos. A natureza isolada das milhares de soluções pontuais oferecidas pelos fornecedores de segurança cibernética faz com que seja quase impossível compreender toda a profundidade e a amplitude da exposição de uma organização.

A complexidade da infraestrutura de TI e sua dependência de vários sistemas em nuvem, diferentes ferramentas de gerenciamento de identidade/privilégios e diversos ativos voltados para a Web, traz consigo inúmeras situações de configurações incorretas e ativos negligenciados.

Em qual das seguintes áreas sua exposição ao risco é mais alta?

Área	Entrevistados
Infraestrutura da nuvem pública	28%
Infraestrutura multinuvem/híbrida	28%
Internet das coisas	16%
Ferramentas de gerenciamento de contêineres na nuvem	12%
Infraestrutura da nuvem privada	10%
Infraestrutura local	6%

BASE: 825 ENTREVISTADOS ENVOLVIDOS NA CONFIGURAÇÃO, NO GERENCIAMENTO E/OU NA IMPLEMENTAÇÃO DE ESTRATÉGIAS, VERBA E/OU MÉTRICAS DE DESEMPENHO DE SEGURANÇA/SEGURANÇA CIBERNÉTICA, INCLUINDO 50 DO BRASIL.

A maioria dos entrevistados (78%) vê a infraestrutura da nuvem, especificamente nuvem pública, multinuvem e/ou híbrida, como a maior fonte de exposição da organização.

Abordar áreas de risco exige não só visibilidade de toda a superfície de ataque, como também a capacidade de analisar as descobertas em contexto e de forma eficaz. No entanto, os líderes de TI e segurança cibernética enfrentam o desafio de extrair perspectivas da miscelânea de ferramentas de segurança cibernética preventiva que estão em uso. Mais de seis em cada 10 entrevistados (62%) usaram 10 ou mais ferramentas de segurança cibernética preventiva nos últimos 12–24 meses.

Quais das seguintes ferramentas/tecnologias sua organização usa como parte da sua estratégia de segurança cibernética?

Ferramentas/Tecnologias	Entrevistados
Criptografia de senhas	88%
Segurança da nuvem	74%
Gerenciamento de identidade e privilégios de usuários	72%
Firewalls	72%
Software antivírus/antimalware	70%
Segurança de comunicação e colaboração (ex.: segurança de e-mail, prevenção contra perda de dados, criptografia)	60%
Detecção e resposta de endpoints (EDR)/ detecção e resposta estendida (XDR)	54%
Gerenciamento de vulnerabilidades	46%
Segurança de aplicações Web	46%
Serviços de segurança gerenciados (ex.: provedores de serviços de segurança gerenciados, MSSP, ou detecção e resposta gerenciadas, MDR)	44%

NOTA: MÚLTIPLAS RESPOSTAS SÃO PERMITIDAS BASE: 825 ENTREVISTADOS ENVOLVIDOS NA CONFIGURAÇÃO, NO GERENCIAMENTO E/OU NA IMPLEMENTAÇÃO DE ESTRATÉGIAS, VERBA E/OU MÉTRICAS DE DESEMPENHO DE SEGURANÇA/SEGURANÇA CIBERNÉTICA, INCLUINDO 50 DO BRASIL.

São necessários vários recursos para gerenciar todas essas ferramentas isoladas. Seis em cada 10 entrevistados (58%) têm 25 ou mais funcionários dedicados à implementação, ao suporte, à manutenção e/ou ao relacionamento com fornecedores das ferramentas de segurança cibernética preventiva em uso.

Para piorar as coisas, os profissionais de TI e segurança cibernética precisam processar muitos dados de muitas fontes diferentes.

Quais das seguintes opções sua organização usa para identificar a exposição geral a riscos?

Fonte de dados	Entrevistados
Descobertas da nuvem	72%
Descobertas da avaliação de prontidão para incidentes	62%
Descobertas de testes de penetração	58%
Feeds de threat intel	56%
Divulgação de vulnerabilidades	52%
Descobertas da superfície de ataque externa	50%
Perfis de usuários e privilégios	42%
Descobertas de tecnologia operacional	30%
Inventário de ativos	22%

NOTA: MÚLTIPLAS RESPOSTAS SÃO PERMITIDAS BASE: 825 ENTREVISTADOS ENVOLVIDOS NA CONFIGURAÇÃO, NO GERENCIAMENTO E/OU NA IMPLEMENTAÇÃO DE ESTRATÉGIAS, VERBA E/OU MÉTRICAS DE DESEMPENHO DE SEGURANÇA/SEGURANÇA CIBERNÉTICA, INCLUINDO 50 DO BRASIL.

Juntar tudo isso é algo complicado e ainda envolve uma outra combinação de ferramentas isoladas, como um SIEM (gerenciamento de eventos e informações de segurança) sofisticado, plataformas de intel de negócios e planilhas de várias guias testadas e aprovadas.

Quais das seguintes opções sua organização usa para coletar e analisar dados a fim de quantificar a exposição geral a riscos?

Método/ferramenta	Entrevistados
Ferramentas de gerenciamento de eventos e informações de segurança (SIEM)	74%
Plataformas de intel de negócios	68%
Ferramentas de agregação	52%
Planilhas de várias guias	38%
Data lake interno próprio da organização	32%

NOTA: MÚLTIPLAS RESPOSTAS SÃO PERMITIDAS BASE: 825 ENTREVISTADOS ENVOLVIDOS NA CONFIGURAÇÃO, NO GERENCIAMENTO E/OU NA IMPLEMENTAÇÃO DE ESTRATÉGIAS, VERBA E/OU MÉTRICAS DE DESEMPENHO DE SEGURANÇA/SEGURANÇA CIBERNÉTICA, INCLUINDO 50 DO BRASIL.

Agregar todos esses dados leva tempo. Leva-se, em média, 14 horas por mês para criar relatórios sobre a integridade da infraestrutura de segurança para os líderes corporativos.

Embora os invasores avaliem os ambientes o tempo todo, na maioria das organizações, reuniões sobre sistemas críticos para o negócio são realizadas com frequência mensal (na melhor das hipóteses!). Um pouco mais do que a maioria (54%) afirma que se reúne mensalmente com os líderes corporativos para discutir quais sistemas são críticos para o negócio, enquanto 22% fazem essas reuniões apenas uma vez por ano e 4% afirmam que nunca fazem reuniões assim.

Sem uma boa compreensão da criticidade dos sistemas que estão em uso, como as organizações podem priorizar suas iniciativas de correção de forma eficaz e reduzir a exposição ao longo do tempo?

A segurança cibernética preventiva requer contexto e visibilidade

As organizações têm o desafio de priorizar as respostas ao escopo completo de exposição da sua superfície de ataque, que vai muito além das vulnerabilidades tradicionais dos softwares de TI e corporativo, incluindo: configurações incorretas nos serviços e na infraestrutura da nuvem, configurações incorretas nas ferramentas usadas para gerenciar acesso e privilégios dos usuários, falhas no código de aplicações Web e falhas no software de tecnologia operacional (OT).

Quais das seguintes situações sua organização considera ser uma exposição e/ou uma vulnerabilidade?

Situação	Entrevistados
Configurações incorretas nas ferramentas que minha organização usa para gerenciar acesso e privilégios dos usuários	78%
Configurações incorretas nos serviços e na infraestrutura da nuvem usados em toda a organização	74%
Falhas em um software de TI/corporativo usado em toda a organização	64%
Falhas em um software de tecnologia operacional usado em toda a organização	36%

NOTA: MÚLTIPLAS RESPOSTAS SÃO PERMITIDAS BASE: 825 ENTREVISTADOS ENVOLVIDOS NA CONFIGURAÇÃO, NO GERENCIAMENTO E/OU NA IMPLEMENTAÇÃO DE ESTRATÉGIAS, VERBA E/OU MÉTRICAS DE DESEMPENHO DE SEGURANÇA/SEGURANÇA CIBERNÉTICA, INCLUINDO 50 DO BRASIL.

Para deixar as coisas ainda mais desafiadoras, as organizações não têm um método padronizado para priorizar a correção de vulnerabilidades em ativos de TI tradicional. Os entrevistados dependem de outros vários aspectos, como metodologias e estruturas, para tentar entender as vulnerabilidades que representam o maior risco para a organização.

Quais dos seguintes métodos sua organização usa para priorizar a correção de vulnerabilidades em ativos de TI tradicional?

Método/estrutura	Entrevistados
Pontuação do Common Vulnerability Scoring System (CVSS)	74%
Documentos do Vulnerability Exploitability eXchange (VEX)	64%
Estrutura do MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)	58%
EPSS	56%
Categorização de vulnerabilidades específica das partes interessadas (SSVC)	38%
Pontuação específica do fornecedor	34%

NOTA: MÚLTIPLAS RESPOSTAS SÃO PERMITIDAS BASE: 825 ENTREVISTADOS ENVOLVIDOS NA CONFIGURAÇÃO, NO GERENCIAMENTO E/OU NA IMPLEMENTAÇÃO DE ESTRATÉGIAS, VERBA E/OU MÉTRICAS DE DESEMPENHO DE SEGURANÇA/SEGURANÇA CIBERNÉTICA, INCLUINDO 50 DO BRASIL.

Embora a maioria dos entrevistados (66%) afirme levar em conta a identidade dos usuários e os privilégios de acesso ao priorizar a correção de vulnerabilidades, mais da metade afirma que a organização não tem uma maneira eficaz de integrar esses dados em suas práticas de gerenciamento de vulnerabilidades. Quase sete em cada 10 (66%) afirmam que seus sistemas isolados constituem uma barreira para a obtenção de dados dos usuários.

Também existem problemas de falta de higiene quando se trata de dados de usuários e sistemas de gerenciamento de vulnerabilidades: 54% dos entrevistados mencionam que é difícil extrair dados de qualidade para respaldar a tomada de decisão de priorização.

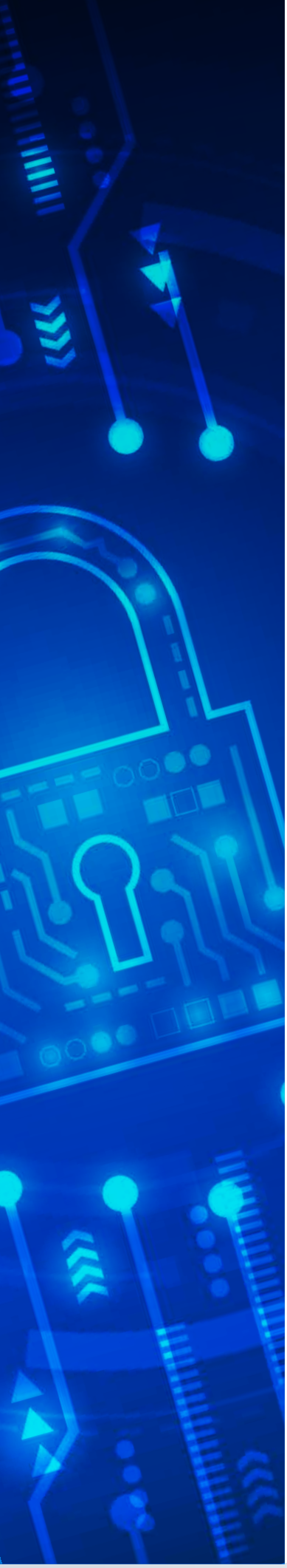
Para piorar as coisas, processos internos e atitudes podem criar conflitos. Por exemplo, quase oito em cada 10 (76%) de todos os entrevistados (profissionais de TI e de segurança) afirmam que a TI está mais preocupada com o tempo de atividade do que com a aplicação de patches/correções.

Além disso, quase metade (46%) dos entrevistados considera a coordenação entre as equipes de TI e segurança cibernética difícil e demorada.

Esses problemas não são novidade. Embora há tempos a aplicação da higiene cibernética básica seja considerada uma forma essencial de reduzir a exposição, continua sendo um desafio para as organizações alcançarem resultados com a combinação existente de ferramentas isoladas.

Enquanto isso, a superfície de ataque cresce exponencialmente e se torna mais complexa ano a ano. A infraestrutura digital moderna abrange diferentes sistemas em nuvem, numerosas ferramentas de gerenciamento de identidade e privilégios, vários ativos voltados para a Web, além de sistemas e softwares de tecnologia operacional (OT) e Internet das Coisas (IoT). O atual ambiente de TI deixa muito espaço para configurações incorretas e ativos negligenciados.

A falta de uma visão unificada e contextual de usuários, sistemas e softwares significa que as equipes de segurança não conseguem avaliar o que está acontecendo na superfície de ataque de forma eficaz. Com interesses concorrentes na empresa, muitas vezes a velocidade e o tempo de atividade ficam à frente da segurança.



Recomendações

No Brasil, as organizações podem começar a reduzir o risco tomando 10 medidas para abordar os desafios de pessoas, processos e tecnologias que estão em seu caminho.

PESSOAS

1. **Repensar a forma como medimos o desempenho das equipes de TI e de segurança cibernética** pode ajudar muito na resolução de conflitos internos e silos na organização. Existem contradições inerentes na forma como cada equipe é recompensada? Considere criar e usar métricas de pontuação e indicadores-chave de desempenho (KPIs) que estejam estreitamente alinhados com o risco cibernético. Todos na organização devem permanecer sob essas mesmas métricas, não importando se trabalham nas equipes de segurança cibernética, TI, engenharia, DevOps, gerenciamento de identidade e acesso ou nuvem.
2. **Reduzir a quantidade de ferramentas isoladas em uso para que as equipes que têm o fardo de gerenciar todas essas soluções discrepantes** (e gastam horas todos os meses reunindo os relatórios) possam focar na análise contínua e na correção preventiva da superfície de ataque, em toda a sua profundidade e amplitude. Dedicar mais recursos à prática de segurança cibernética preventiva é o primeiro passo para reduzir o risco cibernético. Ao avaliar uma nova ferramenta, considere o tempo de obtenção de valor; cada ferramenta nova tem uma curva de aprendizado que diminui a produtividade.

PROCESSOS

3. **Trate a segurança cibernética como uma verdadeira parceira de negócios**, a incluindo o quanto antes no processo de compra e implementação de novas soluções. Permita que a segurança cibernética tenha uma cadeira cativa na definição da estratégia do negócio. A área de segurança cibernética deve trabalhar em estreita colaboração com os líderes corporativos para estabelecer como incorporar métricas de risco cibernético em todos os processos da tomada de decisão. Segurança é um esporte em equipe — não pertence apenas à área de segurança cibernética. A segurança deve ser incorporada em todos os processos do negócio e deve ser gerenciada por todos na organização. As áreas de segurança cibernética e gerenciamento de riscos podem prover estruturas e governança, mas as decisões relacionadas a níveis aceitáveis de risco são, em última instância, tomadas pelas linhas do negócio.
4. **Procure agregar e analisar descobertas discrepantes de segurança cibernética para obter uma compreensão contextual de quais vulnerabilidades e configurações incorretas representam o maior risco para a organização.** Implemente uma abordagem clara e padronizada para priorizar as iniciativas de correção e incentivar as equipes de TI a priorizar a correção com métricas claramente compreendidas e que possam ser rastreadas ao longo do tempo. Se a aplicação de patches não for uma opção, por exemplo, em ambientes de OT ou no caso de indisponibilidade de um patch, considere colocar algum tipo de controle de compensação para reduzir a exposição.

5. **Incorpore segurança de terceiros como parte do programa geral de segurança cibernética.** Implementar um processo pelo qual seja avaliado o acesso aos dados por terceiros e, simultaneamente, sejam realizadas avaliações contínuas do ambiente em busca de ativos não gerenciados conectados à rede corporativa.
6. **Invista na melhoria da higiene de dados em toda a organização.** Sua segurança cibernética está nivelada com os seus dados. A qualidade dos seus dados pode erguer ou derrubar todas as outras iniciativas de segurança cibernética. Com o advento de ferramentas de inteligência artificial generativa, a qualidade dos dados nunca foi tão importante. Como diz o ditado, "lixo entra, lixo sai".
7. **Implemente KPIs para monitorar e mensurar a eficácia dos seus processos.**

TECNOLOGIAS

8. **Audite seu atual conjunto de ferramentas.** Você consegue agregar e analisar as descobertas da sua superfície de ataque, em toda a sua profundidade e amplitude, de forma rápida e eficaz, incluindo gerenciamento de vulnerabilidades, segurança de aplicações Web, segurança da nuvem, segurança de identidade, análise das vias de ataque e gerenciamento de superfície de ataque? Se for difícil obter uma avaliação precisa e contextual de toda a profundidade e a amplitude da sua superfície de ataque, qualquer que seja o momento, talvez seja hora de uma nova abordagem.
9. **Reavalie todas as suas ferramentas isoladas de segurança cibernética e as funções que elas desempenham.** Quais são usadas sobretudo em respostas reativas a incidentes e quais ajudam você a praticar a segurança cibernética preventiva no dia a dia? As ferramentas estão criando silos internos que impedem a comunicação e a coordenação eficazes entre as áreas de TI e segurança cibernética? As ferramentas preventivas e de resposta a incidentes também devem ser integradas; uma pode enriquecer a outra com um contexto importante.
10. **Audite o valor das informações que você coleta.** Você consegue determinar rapidamente a relação entre usuários, sistemas e softwares na organização para que seja possível identificar e abordar sua exposição de forma realista? Ou será que os sistemas isolados formam uma barreira que impede a integração eficaz desses dados nas suas práticas de gerenciamento de exposição? Ao reunir mais dados de várias fontes, como nuvem, sistemas de OT, ferramentas de gerenciamento de acesso e identidade, verificadores de aplicações Web e ferramentas de gerenciamento de superfície de ataque, corre-se o risco de sobrecarga de dados. A higiene de dados é crucial, mas não é a única peça do quebra-cabeça que deve ser considerada. Também é necessário considerar cuidadosamente a plataforma que está sendo usada e se ela pode ajudar a encontrar algumas agulhas críticas no famigerado palheiro, que aumenta exponencialmente ano a ano.

O caminho para o gerenciamento de exposição

Para proteger os ambientes de TI complexos e dinâmicos dos dias de hoje, é preciso reunir gerenciamento de vulnerabilidades, segurança de aplicações Web, segurança da nuvem, segurança de identidade, análise das vias de ataque e gerenciamento de superfície de ataque externa para ajudar a entender a amplitude completa da sua exposição. A complexidade da superfície de ataque moderna é o grande fator por trás do surgimento de programas de gerenciamento de exposição. As equipes de segurança têm o desafio de acompanhar o fluxo constante de dados da grande variedade de soluções pontuais que elas usam para gerenciar vulnerabilidades, aplicações Web, sistemas de identidade e ativos de nuvem. E têm o desafio de analisar todos esses dados com eficácia para tomar decisões embasadas e proativas de quais exposições representam o maior risco para a organização. A implementação de um programa de gerenciamento de exposição permite que os profissionais de segurança aloquem melhor o tempo e os recursos para poderem focar em medidas preventivas que reduzam legitimamente o risco cibernético da organização.

A adoção de um programa de gerenciamento de exposição envolve mudanças de processos e pessoas. Exige que as equipes de segurança atribuam às iniciativas proativas a mesma importância que atribuem às atuais iniciativas reativas de resposta a incidentes. Exige que os profissionais de TI e segurança considerem como as estruturas organizacionais isoladas — e as inúmeras ferramentas de segurança usadas como suporte a esses silos — atrapalham sua capacidade de ver o que o invasor vê. E, por fim, exige uma forma pela qual os profissionais de segurança possam analisar os dados provenientes de ferramentas diferentes para obter informações relevantes que possam ser aplicadas às suas metas de redução de risco.

O gerenciamento de exposição permite que a organização entenda o risco cibernético para que você possa tomar decisões mais eficazes para o negócio. Fundamentado no gerenciamento de vulnerabilidades baseado em riscos, o gerenciamento de exposição tem uma visão mais ampla em sua superfície de ataque moderna, aplicando contexto técnico e do negócio para identificar e comunicar mais precisamente o risco cibernético, permitindo melhores decisões para o negócio.

SOBRE A TENABLE

A Tenable® é a empresa de Exposure Management. Aproximadamente 43 mil organizações no mundo todo contam com a Tenable para entender e reduzir o risco cibernético. Como criadora do Nessus®, a Tenable ampliou sua experiência em vulnerabilidades para oferecer a primeira plataforma do mundo para verificar e proteger qualquer ativo digital em qualquer plataforma de computação. Entre os clientes da Tenable, estão 60% das empresas Fortune 500, 40% das empresas Global 2000 e órgãos governamentais de grande porte.

Saiba mais em **pt-br.tenable.com**

Publicação/Velhos hábitos nunca morrem/02/11/23