Guia para líderes

FAZENDO AVANÇOS COM A SEGURANÇA MODERNA:

como os CIOs podem aprimorar a resiliência cibernética

Uma das maiores prioridades para os CIOs agora é a segurança cibernética.

A recente aceleração rápida da transformação digital e do trabalho distribuído mudou o cenário da segurança cibernética.

Quando a maioria dos funcionários trabalhava exclusivamente em um escritório, os limites da segurança cibernética eram mais claros. Com o trabalho remoto, a superfície de ameaças se expande para onde quer que seus funcionários estejam.

No "Breakthrough Study" da Dell Technologies, baseado em uma pesquisa com mais de 10,5 mil pessoas de mais de 40 locais,

72% dos entrevistados disseram que o mundo do trabalho em constante mudança expõe a organização deles a um maior risco de segurança cibernética.

O desafio que os CIOs enfrentam está na interseção de medidas eficazes de segurança cibernética e as realidades da vida. Quase dois terços dos entrevistados (62%) disseram que seus funcionários são o elo mais fraco do ambiente de segurança. Os funcionários confirmam essa preocupação, uma vez que mais da metade (56%) afirma que não mudaram muito sua abordagem ou comportamento de segurança, mesmo com maior conscientização sobre os riscos.

Esse é um problema universal e humano: até mesmo a pessoa mais preocupada com a segurança está propensa a deslizes. A estratégia mais eficaz não é intimidar os funcionários a aderir a protocolos existentes e potencialmente desatualizados, mas garantir que sua postura de segurança leve em consideração o fator humano.

Como CIO, você é responsável por proteger inúmeros locais inseguros. Embora seus funcionários possam ajudar um pouco, contar apenas com a participação deles não será suficiente. Essa responsabilidade pode parecer assustadora, mas não é algo impossível.

Veja o que você precisa saber para manter a segurança dos funcionários e da infraestrutura de TI.

Os cinco principais motivos pelos quais os entrevistados acreditam que suas equipes são vítimas de ataques cibernéticos:

1. Excesso de confiança nos firewalls da organização para impedir ameaças
2. Subestimação da escala da ameaça
3. Esperança de que eles não serão alvos
4. Suposição de que os efeitos negativos são fáceis de reverter
5. Desconsideração da ameaça por não saberem resolvê-la

“A segurança é responsabilidade de todos. Com a crescente ameaça à segurança, as empresas precisam equipar seus funcionários com o conhecimento certo e uma compreensão de que podem ajudar a impedir criminosos cibernéticos ao seguir os requisitos de segurança que a organização estabeleceu. As empresas também devem tornar esse comportamento o padrão por meio da implementação de tecnologias e processos de tecnologia intrinsecamente seguros. É fundamental integrar a mensagem de responsabilidade de segurança compartilhada na cultura. Geralmente, as pessoas precisam ouvir uma mensagem várias vezes, de maneiras diferentes, antes disso se transformar em um comportamento.”

John Scimone, vice-presidente sênior e diretor de segurança, Dell Technologies

Prevenção do comportamento inseguro

CIOs e CISOs são responsáveispor implantar tecnologia para proteger os ativos digitais da empresa. Mas o que acontece quando as partes mais inseguras (e voláteis) do sistema são as pessoas que o usam?

Mesmo com as melhores intenções, o erro humano é inevitável. É por isso que é importante ter um plano para quando, e não se, suas medidas de segurança cibernética forem submetidas ao teste derradeiro de um ataque de segurança cibernética real. Esse plano requer uma solução escalável e responsiva que proporcione o seguinte:

1. **Proteção de dados e sistemas:** a solução deve proteger os funcionários onde quer que eles estejam trabalhando, independentemente do dispositivo utilizado.
2. **Aprimoramento da resiliência cibernética:** camadas de recursos de segurança e recuperação de desastres são componentes essenciais.
3. **Superação da complexidade da segurança:** uma solução simplificada e fácil de usar ajudará a aumentar a conformidade.

Como CIO, cabe a você fortalecer suas tecnologias de negócios e confiar nas pessoas que dependem delas. Para isso, é necessário responder a algumas perguntas importantes:

- A segurança cibernética da sua organização abrange todo o ecossistema de TI, inclusive dispositivos, aplicativos e sistemas?
- Como você evita o comportamento inseguro do usuário final? Por exemplo, você usa um software de otimização baseado em IA para automatizar os controles de privacidade quando o usuário se afasta de seu dispositivo?
- Sua organização avaliou os riscos novos e possivelmente maiores trazidos pelo trabalho remoto?

Proteção de dados e sistemas

A complexidade e os silos inerentes a uma força de trabalho distribuída multiplicam a vulnerabilidade a ataques cibernéticos. Dados exclusivos estão em risco sempre que são enviados entre nuvens e ambientes de trabalho remoto.

Essas vulnerabilidades podem ser eliminadas com um modelo de segurança completo que supera os silos e a complexidade, como Zero Trust.

O Zero Trust é um modelo de segurança de TI baseado no conceito de que nenhuma interação deve ser confiável e, portanto, todas as interações devem ser verificadas. Esse modelo de autenticação em cada etapa pode ser aplicado na rede, infraestrutura de TI, software e microsserviços da sua organização.

Com uma abordagem Zero Trust em várias camadas, um perímetro é criado em torno de cada interação. Mesmo que um agente de ameaça cruze um perímetro, ele não poderá explorar uma suposição de confiança com base no acesso atual ao sistema. Cada gateway que ele tentar passar exigirá autenticação. Esses protocolos de segurança "negados por padrão" podem ajudar a proteger os dados, desenvolver a confiança dos funcionários e criar relacionamentos confiáveis com seus clientes.

Ao começar a fortalecer os sistemas da sua organização para proteger aplicativos e dados, considere estas questões cruciais:

- Sua postura geral de segurança está de acordo com o modelo Zero Trust?
- Seus fornecedores e a equipe interna de DevOps têm medidas apropriadas de segurança cibernética em vigor para garantir um ciclo de vida de desenvolvimento seguro que proteja os processos pelos quais novos produtos, recursos e serviços são desenvolvidos/implementados?
- Seu recurso de segurança atual está incluído ou integrado? Isolado ou unificado? Centrado em ameaças ou centrado em contexto?

Preservar seus dados é onde e como seus dados de backup são armazenados. Antes de comprometer seus dados principais, os invasores cibernéticos geralmente tentam comprometer seus backups.

Aprimoramento da resiliência cibernética

Como diz o ditado, **"A única coisa mais difícil do que se planejar para um desastre é explicar por que você não fez isso".**

O fundamental para alcançar a resiliência cibernética é presumir que um ataque ocorrerá e tomar medidas prospectivas para se recuperar o mais rápido possível, com impactos financeiro e operacional mínimos.

Essas etapas incluem a realização de simulações que testam os sistemas de continuidade e recuperação de negócios e operacionais, bem como sua resposta de segurança cibernética e resposta corporativa em funções-chave, como jurídico, gerenciamento de crises e comunicações.

No entanto, esse tipo de teste rigoroso pode ser demorado. Uma solução gerenciada pode livrar sua equipe dessas tarefas e identifica as ameaças e tendências emergentes em ataques cibernéticos. Por exemplo, um serviço gerenciado de detecção e resposta a ameaças examina as ameaças e investiga as respostas de sua empresa para você.

Outra consideração importante é preservar seus dados, o que significa saber onde e como seus dados de backup são armazenados. Antes de comprometer seus dados principais, os invasores cibernéticos geralmente tentam comprometer seus backups.

A melhor defesa contra isso é uma cópia isolada e off-line de seus sistemas essenciais. A história da Founders Federal Credit Union (FFCU) mostra como e por que isso pode ser feito.

A FFCU calculou que, caso um ataque cibernético como o ransomware acontecesse, eles teriam uma janela de uma hora para recuperar seus dados e retomar as operações. Isso os levou a realizar uma grande reformulação da segurança cibernética do data center com foco em voltar a funcionar rapidamente. Eles implementaram um compartimento de recuperação cibernética, que fica atrás de um "air gap" operacional que o mantém separado do sistema e, ao mesmo tempo, sincroniza regularmente os dados de produção. Isso permite que a FFCU garanta que os dados estarão sempre disponíveis, protegidos e não corrompidos.

Ao procurar reforçar sua resiliência cibernética em um ambiente de segurança em evolução, considere estas questões:

- Sua organização determinou o tempo durante o qual suas operações seriam interrompidas no caso de um ataque cibernético?
  - Em caso afirmativo, são minutos, dias ou semanas?
- Quando foi a última vez que você identificou cargas de trabalho e dados essenciais aos negócios para colocar em proteção isolada?
- Que tipo de recursos de detecção de ameaças você tem em vigor?
  - Eles são gerenciados internamente ou por terceiros?
  - Sua organização utiliza a detecção de anomalias de padrão baseada em IA?

A complexidade é inimiga da segurança

Quando a equipe de operações de segurança gerencia soluções para sua ampla variedade de componentes de infraestrutura de TI, a complexidade e, portanto, o risco podem aumentar rapidamente. Com essa complexidade, também vem o aumento dos custos e da ineficiência em suas operações regulares. Geralmente, para encontrar um equilíbrio entre eles, é preciso fazer concessões insustentáveis em ambas as frentes.

Há um modo melhor de dimensionar sua operação de segurança cibernética. Você pode liberar tempo e recursos com ferramentas avançadas de segurança que usam inteligência artificial (IA) e aprendizado de máquina (ML) para permitir governança e comportamento mais consistentes.

As ferramentas de IA ajudam suas soluções de detecção de ameaças a identificar e relatar anomalias na rede, bem como violações de políticas, o que iniciaria uma série de ações de segurança. A segurança automatizada também pode melhorar o código de desenvolvimento de software. Com menos falhas e erros humanos, surgem menos vulnerabilidades.

No entanto, para obter o máximo valor de suas ferramentas de segurança, você precisa que elas sejam fáceis de usar e gerenciar. Ao consolidar os aplicativos e parceiros de segurança de sua organização, você obterá mais controle e simplificará o gerenciamento de TI para que suas equipes de TI possam se concentrar na inovação. Os serviços gerenciados podem ser uma ótima forma de aproveitar as melhores e mais recentes tecnologias de segurança, além de aliviar as cargas de trabalho das equipes internas, mas é importante selecionar cuidadosamente e racionalizar os fornecedores quando possível. Escolha um parceiro de confiança que não só entenda seus desafios únicos, mas também que possa amplificar os recursos de suas equipes de TI com serviços de segurança cibernética para que você possa manter a eficiência à medida que evolui.

Ao planejar agilizar as operações sem diminuir suas defesas, considere estas questões:

- Sua organização garante o nível apropriado de redundância em seu recurso de segurança?
- Sua organização usa ferramentas de IA para ajudar na detecção, resposta e recuperação?
- Sua organização examina rotineiramente seus provedores de segurança internos e de terceiros para garantir a eficácia e o valor?

Um mundo remoto requer segurança mais inteligente

Dados distribuídos, modelos de trabalho remoto, ambientes multicloud e fornecimento as a service apresentam incertezas significativas no ambiente moderno de segurança cibernética. O erro humano pode agravar essa incerteza. Como CIO, cabe a você garantir que sua segurança cibernética seja responsável por cada uma dessas incertezas.

Uma abordagem moderna de segurança cibernética é vital. Seu equipamento de segurança cibernética precisa estar preparado para proteger seus dados e sistemas, reduzir o impacto dos ataques cibernéticos e dimensionar as medidas de segurança cibernética de forma eficaz, minimizando a complexidade adicional.

A Dell Technologies tem o compromisso de ajudar você a planejar, proteger, detectar, responder e se recuperar de ataques cibernéticos para que seus recursos e suas equipes possam se dedicar totalmente ao que importa: impulsionar seus negócios.

Saiba mais em dell.com/cio

Saiba mais sobre o "Breakthrough Study" em dell.com/breakthrough

Saiba mais sobre nossas soluções de segurança em:
dell.com/en-us/dt/solutions/security/index.htm

Fonte: Com base em "The Breakthrough Study" da Dell Technologies de abril de 2022. Trabalho de campo realizado de agosto a outubro de 2021. Pesquisa e análise conduzidas pela Vanson Bourne em nome da Dell Technologies.

DELL Technologies