O guia de sobrevivência para a segurança cibernética:

Como responder às ameaças cibernéticas modernas

O mundo digital se tornou um ambiente selvagem, onde cada clique, download ou log-in pode acionar uma armadilha cibernética oculta.

O cenário cibernético de hoje está mais perigoso do que nunca, com ameaças como ransomware, ataques DDoS, tentativas de phishing e infiltrações de backups se tornando cada vez mais sofisticadas. Os hackers agora utilizam a IA para superar as defesas tradicionais, transformando o que antes eram ataques oportunistas em ameaças calculadas e persistentes, capazes de causar danos generalizados.

Os clientes da Dell relataram ataques alarmantes baseados em IA, nos quais hackers vasculham as mídias sociais para criar mensagens convincentes que podem enganar até mesmo os funcionários mais informados sobre ataques cibernéticos.

Essas histórias são um lembrete claro de como os invasores estão explorando tecnologias avançadas para manipular, enganar e se infiltrar em organizações com precisão sem precedentes.

Para navegar neste ambiente hostil, as organizações precisam de uma estratégia abrangente de segurança cibernética, um kit de sobrevivência que combina ferramentas de ponta, estratégias proativas e uma cultura de vigilância. Este guia explora os componentes dessa estratégia, ajudando as organizações a desenvolver resiliência contra as ameaças cibernéticas mais urgentes da atualidade.

O mapa para proteger sua organização: uma estrutura Zero Trust

No cenário atual de ameaças impulsionadas pela IA, adotar uma estrutura Zero Trust não é mais opcional. Os invasores estão usando a IA para automatizar o reconhecimento, roubar credenciais e adaptar suas técnicas rapidamente, tornando as defesas tradicionais menos eficazes. A estrutura Zero Trust opera com uma mentalidade de "presumir que ocorrerá uma violação", verificando continuamente cada solicitação de acesso e implementando processos de autenticação rigorosos para minimizar riscos.

Ao monitorar proativamente usuários, dispositivos e aplicativos, a abordagem Zero Trust reduz a probabilidade de acesso não autorizado e de violações de dados. É uma abordagem moderna e unificada para gerenciamento de identidades.

Planejamento e proatividade: Reduza a superfície de ataque

Reduzir a superfície de ataque é essencial para se defender contra ameaças orientadas por IA, com vulnerabilidades de endpoints, APIs e cadeia de suprimentos frequentemente exploradas por invasores. Os endpoints e as APIs servem como pontos de entrada para redes e frequentemente são alvos para implementação de malware ou roubo de dados confidenciais.

A proteção dessas áreas exige uma estratégia de defesa em camadas, incluindo autenticação forte, criptografia de dados em trânsito, testes regulares de vulnerabilidade, ferramentas de detecção e resposta de endpoint (EDR), gerenciamento de patches e fortalecimento de dispositivos. Soluções de monitoramento de endpoints e detecção contínua de ameaças ajudam a identificar e bloquear atividades mal-intencionadas em tempo real.

As organizações devem adotar estratégias proativas para proteger as cadeias de suprimentos de software e o ciclo de vida de desenvolvimento. Impor o acesso com privilégios mínimos garante que somente usuários e aplicativos autorizados possam interagir com sistemas essenciais, enquanto a detecção e a resposta automatizadas de ameaças podem abordar vulnerabilidades rapidamente à medida que elas surgem.

Siga e aprenda com um especialista: Detecção proativa de ameaças e resposta

Os ataques baseados em IA exploram vulnerabilidades, imitam comportamentos legítimos e se adaptam dinamicamente para contornar medidas de segurança, dificultando sua detecção. Para combater essas ameaças sofisticadas, as organizações precisam de mais do que medidas reativas, elas exigem sistemas de detecção de ameaça avançada, combinados com recursos de resposta rápida. Ao utilizar a IA e o aprendizado de máquina, as equipes de segurança podem analisar padrões comportamentais, detectar anomalias e responder a ameaças em tempo real, abordando problemas antes que danos significativos ocorram.

Um sistema eficaz de detecção e resposta precisa processar grandes volumes de dados operacionais para identificar riscos e acionar respostas automatizadas. Essa inteligência contra ameaças também se aprimora continuamente, tornando o sistema mais inteligente e capaz de identificar e neutralizar proativamente novas táticas de adversários.

É melhor prevenir do que remediar: resposta e recuperação a incidentes

Embora prevenir ataques seja o primeiro passo, as organizações devem operar como se um ataque fosse inevitável. O objetivo é sobreviver ao ataque com dano mínimo, e uma estratégia eficaz envolve duas partes:

- Um plano sólido de Resposta e recuperação de incidentes (IRR).
- Medidas tecnológicas centradas no backup de dados e aplicativos críticos.

Um plano de recuperação de incidentes deve ser abrangente. Como um ataque poderoso provavelmente derrubará a maioria das operações da empresa, se não todas, o plano deve abranger o que cada departamento da empresa faria no caso de um incidente cibernético. O plano também deve abordar como a organização se comunicará interna e externamente, com modelos de comunicação pré-escritos e prontos para uso. O plano também deve ser atualizado e mantido regularmente. Por fim, o plano só é bom na medida em que é praticado. Quando o ataque ocorre, todos devem estar instintivamente prontos para agir.

Da perspectiva tecnológica, as organizações devem começar determinando como são as operações da **Empresa Mínima Viável (MVC):** Quais sistemas DEVEM permanecer operacionais, mesmo que isso signifique ficar sem papel e lápis? É essencial que as vendas continuem funcionando? E quanto ao atendimento ao cliente?

Uma vez que essas determinações forem feitas, os mecanismos de backup e recuperação devem ser criados em torno delas. Ter a capacidade de reverter para dados íntegros previamente conhecidos não apenas permite que a organização retome rapidamente suas operações, como também retira a vantagem de agentes mal-intencionados que tentam manter seus dados como reféns. Além disso, as estratégias modernas de resposta a incidentes (IR) devem ir além das abordagens tradicionais, tratando sistemas de IA/LLM como chatbots e agentes virtuais, como ativos de Nível 1 com a mesma prioridade de recuperação que os sistemas de pagamento ou de dados do cliente.

Para combater ameaças avançadas, os planos de resposta a incidentes devem equilibrar a automação com verificações manuais. É essencial saber como sua organização funcionará no caso de uma interrupção total do sistema. E se você tiver que voltar a usar papel e caneta?

Todos precisam colaborar: Conscientização dos funcionários

Os funcionários são a primeira linha de defesa contra ameaças cibernéticas, assim como uma equipe de sobrevivência que enfrenta os perigos na natureza. Cada membro desempenha um papel fundamental na identificação de riscos e na proteção de recursos. Para fortalecer essa defesa, as organizações precisam de programas robustos de conscientização, incluindo simulações de ataques que contemplem ameaças específicas de IA, como phishing avançado e deepfakes.

Os melhores programas combinam educação contínua, comunicação aberta, simulações do mundo real e uma cultura de responsabilidade compartilhada. Quando todos, desde a equipe da linha de frente até os executivos, entendem as ameaças tradicionais e as baseadas em IA, a organização se torna uma unidade vigilante e bem-informada. Ao promover o trabalho em equipe e a preparação, sua organização pode ficar à frente dos riscos cibernéticos em evolução e criar uma defesa resiliente contra possíveis ataques.

Melhores práticas para permanecer resiliente contra ataques orientados por IA

Para permanecerem resilientes contra ataques baseados em IA, as organizações precisam adotar uma abordagem proativa e estratégica. Aqui estão as 10 melhores práticas:

Arquitetura Zero Trust

Exija verificação contínua, controles de acesso rigorosos e segmentação de rede para garantir que cada usuário e dispositivo seja autenticado antes de conceder acesso, ajudando a bloquear e conter ataques em rápida evolução e baseados em IA.

Fortalecendo o gerenciamento de acesso e de identidades:

Implemente autenticação robusta (MFA, RBAC) e aplique políticas de credenciais sólidas para reduzir o sucesso de ataques de phishing e preenchimento de credenciais.

Inventário e detecção automatizada de ativos:

Detecte e monitore continuamente todos os ativos, incluindo nuvem, IoT e TI invisível, para evitar exposições ocultas.

Controles de acesso à rede e microssegmentação:

Segmente e isole redes e cargas de trabalho para impedir o movimento lateral de invasores e conter ameaças.

Fortalecimento de API e endpoint:

Use proteção avançada de endpoints (EDR/XDR) e gateways de API seguros; autenticação robusta, limitação de taxa, validação de entrada e criptografia.

Gerenciamento rigoroso de patches e vulnerabilidades:

Automatize a verificação e a aplicação rápida de patches de sistema operacional, firmware, aplicativos, APIs e software de terceiros.

Detecção e monitoramento de ameaças orientados por IA:

Aproveite a detecção de anomalias e comportamental com tecnologia de IA/ML para identificar ameaças sutis ou automatizadas em tempo real.

Resposta automatizada a incidentes:

Use guias estratégicos de reprodução automatizados para isolar, conter e corrigir ameaças rapidamente, minimizando o tempo de permanência dos invasores.

Simulações realistas regulares e melhoria contínua:

Realize exercícios de mesa, red teaming e simulações de phishing; atualize os planos de resposta a incidentes (IR) e os modelos de detecção com base nos resultados.

Backups com air gap imutáveis e recuperação:

Mantenha backups invioláveis, de preferência com air gap e testados regularmente, para garantir recuperação rápida e limpa.

DELL Technologies

Dell Technologies: Seu guia através do território desconhecido

Proteger sua organização contra ameaças cibernéticas avançadas requer conhecimento e ferramentas certas para ficar à frente dos riscos em evolução. No complexo cenário de segurança cibernética atual, uma estratégia robusta é essencial para proteger seus dados, sistemas e reputação. É aí que a Dell Technologies entra, oferecendo um conjunto abrangente de soluções personalizadas para atender às necessidades de organizações de todos os portes.

Desde uma cadeia de suprimentos segura, detecção de ameaça avançada e proteção de endpoints até o gerenciamento seguro de dados, a Dell equipa sua empresa com a tecnologia necessária para se defender dos ataques cibernéticos modernos. Com o apoio do conhecimento líder do setor, a equipe da Dell trabalha em estreita colaboração com você para desenvolver uma estratégia de segurança personalizada. Com recursos como monitoramento em tempo real, resposta automatizada a ameaças e arquitetura Zero Trust, a Dell ajuda a garantir que sua organização permaneça proativa e resiliente.

Não importa se você está lidando com ransomware, ataques de phishing ou conformidade regulatória, a Dell Technologies ajuda você a navegar pelo cenário de ameaças atual com confiança. Faça parceria com a Dell para proteger seu negócio e prosperar na era digital, garantindo que suas operações estejam seguras, eficientes e prontas para o que vier.

> "Seu plano de resposta a incidentes deve ser impresso em papel, pois seus sistemas podem ficar inacessíveis durante um ataque."
>
> ***Rachel Tyler***
> *Consultoria e assessoria de segurança cibernética, serviços Dell*

Produtos e soluções da Dell que podem ajudar

Solução Dell em destaque	Descrição
Infraestrutura confiável da Dell	Uma combinação de servidores, redes, armazenamento e soluções de resiliência cibernética da Dell que, juntos, criam uma base moderna, segura e resiliente para a inovação.
Resiliência cibernética	Um portfólio abrangente de soluções projetadas para proteger seus dados e garantir uma recuperação segura. Inclui equipamentos, software e ofertas "as a service".
Serviços de segurança cibernética	Um conjunto de serviços que pode ajudar você a desenvolver e implementar uma estratégia de segurança abrangente para todas as cargas de trabalho. As ofertas incluem serviços de consultoria, vCISO, Managed Detection and Response, testes de violação e vulnerabilidade, e resposta e recuperação de incidentes.
Dell Trusted Workspace (Segurança de endpoints)	Uma combinação de recursos nativos e opcionais adicionais projetados para proteger PCs comerciais. Desenvolvida com práticas seguras na cadeia de suprimentos, os recursos integrados incluem SafeBIOS e SafeID com TPM. Os complementos opcionais incluem Secured Component Verification, SafeID com ControlVault e software de parceiros como CrowdStrike e Absolute para maximizar a segurança do espaço de trabalho.

Saiba como enfrentar alguns dos principais desafios atuais de segurança cibernética em **dell.com/cybersecuritymonth**

DELL Technologies