ActualTech MEDIA

Hewlett Packard Enterprise

Fique preparado para as ameaças de segurança

Ed Tittel

CONTEÚDO

NESTE DOCUMENTO

Este resumo técnico analisa como a HPE e seus parceiros ajudam pequenas e médias empresas a evitar problemas de segurança. Essas operações devem ser capazes de identificar ameaças e vulnerabilidades que representam riscos potenciais, priorizá-las por gravidade e definir planos de ação e mitigação de riscos para abordá-los. Isso envolve um esforço constante e contínuo para acompanhar um cenário de ameaças em constante mudança.

Estes são os destaques:

- Alinhamento da estratégia de segurança com os objetivos de negócios
- Construção de uma cultura de negócios que prioriza a segurança
- Monitoramento de superfícies de ataque e remediação proativa antes que hackers consigam atacar

Quando se trata de segurança cibernética, o velho ditado "é melhor prevenir do que remediar" é particularmente adequado. Isso porque os custos do tratamento – remediar as consequências de um incidente ou violação de segurança – são altos o suficiente hoje em dia para representar uma ameaça à existência da maioria das empresas, especialmente operações menores.

É isso que torna tão importantes, se não absolutamente essenciais, a compreensão e a antecipação dos perigos que as ameaças e vulnerabilidades de segurança podem representar. Em última análise, trata-se de gerenciamento de riscos, o que significa o seguinte:

- À medida que as ameaças e vulnerabilidades se tornam conhecidas, o primeiro passo é **identificar** aquelas que representam riscos reais para o negócio e avaliar seus potenciais impactos e consequências.
- Para os itens em que há risco envolvido, é essencial **priorizá-los** para que aqueles com os custos mais altos ou as consequências mais terríveis sejam abordados primeiro, e assim por diante, em ordem decrescente.
- Para itens com risco suficiente para justificar uma resposta, as empresas devem estabelecer **mitigação de riscos e planos de ação** para abordá-los.

Na prática, especialmente para empresas muito pequenas para implementar uma equipe de segurança interna, isso significa assinar algum tipo de serviço de inteligência e remediação de ameaças. A HPE e seus parceiros podem ajudar com isso, incluindo identificação, priorização e correção de riscos como parte de uma oferta abrangente de serviços de segurança.

A nuvem muda tudo... inclusive a segurança

À medida que as organizações passam a utilizar assinaturas e serviços de nuvem, novos e desafiadores vetores de ameaças também entram no quadro de segurança de uma empresa. Isso torna vital melhorar as ações de segurança e tomar medidas para melhorar a postura de segurança da organização e a resiliência cibernética. As seguintes medidas de negócios devem ser tomadas para ajudar as empresas a atingir esses objetivos:

- **Alinhe sua estratégia de segurança com suas prioridades de negócios:** Ao entender as lacunas entre as prioridades de negócios e de segurança cibernética, a administração e as partes interessadas podem começar a alinhar ambas as estratégias para garantir que as prioridades mais altas permaneçam focadas e que os recursos e orçamentos sejam alocados de acordo. É importante que os líderes de negócios cheguem a um acordo sobre as prioridades e que os perfis de risco sejam entendidos com clareza.
- **Crie uma cultura de prioridade para a segurança:** Priorizar uma cultura de prioridade para segurança é um passo importante para prosperar em um mundo repleto de incertezas e riscos. Proteger ativos vitais torna-se uma responsabilidade de todos. É essencial investir em treinamento de conscientização da equipe, devido ao seu destaque como fonte de risco cibernético e porque um esforço coletivo contra ameaças cibernéticas servirá melhor ao seu negócio.
- **Conheça sua superfície de ataque e corrija as vulnerabilidades antes que os hackers as encontrem:** A análise de vulnerabilidade cibernética, também chamada de teste de segurança ou teste de caneta, é um processo de teste para avaliar a postura de segurança da sua organização (consulte a **Figura 1**). Ela identifica vulnerabilidades antes que um invasor possa explorá-las. Esse processo fornece insights sobre os riscos que os ativos organizacionais enfrentam, a partir de perspectivas externas e internas. Também ajuda a identificar possíveis falhas de segurança antes de avaliações ou auditorias formais de conformidade. Para aprimorar a postura de segurança em sua organização, também é importante desenvolver planos de mitigação que possam ser postos em prática. Para isso, envolver parceiros experientes (como a HPE e seus parceiros) pode preencher as lacunas de habilidades cibernéticas em seus negócios e mitigar vulnerabilidades.

Quatro estágios de teste de invasão

Figura 1: Os quatro estágios do teste de invasão, também conhecido como teste de caneta

Explicação da terminologia

Recuperação de desastres: Descreve serviços e sistemas que permitem que uma empresa retorne à operação normal mesmo em caso de desastre ou interrupção total de acesso e serviço.

Ransomware: Um tipo de malware que nega às empresas o acesso aos seus sistemas e dados, criptografando tudo para que nada funcione. Os bandidos afirmam que o pagamento de um resgate retornará tudo a um estado pré-ataque, mas o FBI recomenda não pagar resgates porque nem sempre é assim que as coisas acontecem.

Aplicativos e dados virtualizados e contentorizados: Aplicativos e dados executados em máquinas virtuais ou contêineres, geralmente na nuvem, normalmente como parte de um modelo de computação baseado em consumo e uso.

Da borda à nuvem: Refere-se a recursos de computação e dados que podem residir em data centers ou salas de servidores no local no núcleo dos negócios, na borda da rede em locais remotos em campo ou em uma ou mais plataformas de nuvem (por exemplo, Amazon Web Services, Microsoft Azure, Google Cloud Platform).

Cenários híbridos e multicloud: Uma nuvem híbrida envolve a integração de recursos de computação locais e baseados em nuvem em um único ambiente para lidar com tarefas de computação. Multicloud significa a mesma coisa, exceto por envolver duas ou mais plataformas de nuvem. A maioria das empresas modernas opera em ambientes híbridos multicloud e procura posicionar cargas de trabalho e dados onde eles fazem mais sentido do ponto de vista de custo, segurança e desempenho.

> **É importante que os líderes de negócios cheguem a um acordo sobre as prioridades e que os perfis de risco sejam entendidos com clareza.**

Como a HPE (e os parceiros) podem proteger a TI

As soluções de segurança cibernética da HPE são abrangentes, inovadoras e robustas, o que pode ser constatado por um exame rápido. Seus recursos de segurança começam no nível do hardware e se estendem até os usuários e sistemas na borda da rede. O objetivo geral é reunir e analisar inteligência de segurança para acompanhar o cenário de ameaças, proteger sistemas e serviços em uso comercial e aconselhar (e ajudar) seus clientes a gerenciar e minimizar os riscos de segurança.

> **As soluções de segurança cibernética da HPE são abrangentes, inovadoras e robustas. Seus recursos de segurança começam no nível do hardware e se estendem até os usuários e sistemas na borda da rede.**

A SEGURANÇA DA HPE COMEÇA COM SEUS SERVIDORES

A HPE é reconhecida como fornecedora dos servidores padrão do setor mais seguros do mundo. Sua linha de servidores ProLiant ganhou inúmeros prêmios e elogios, graças a essas características específicas:

- **Proteção:** Os sistemas evitam a exposição de nível de hardware e firmware a ataques por meio de uma root of trust de silício, aprimoramentos de módulo de plataforma confiável (TPM), vários níveis de inviolabilidade e inovações adicionais da HPE, como firmware "Integrated Lights Out" (iLO) para promover capacidades de "prioridade para segurança".
- **Detecção:** Um conjunto completo de inovações detecta e afasta ameaças durante o tempo de execução, incluindo verificações de integridade de inicialização, em que o iLO limpa o código de firmware potencialmente (ou realmente) invadido e o substitui por uma cópia válida conhecida, se possível. Se o reparo for impossível, os sistemas não poderão inicializar (fornece proteção pré-inicialização contra rootkits e outros ataques traiçoeiros baseados em firmware).

- **Recuperação:** Recursos robustos para restaurar e recuperar sistemas de volta aos seus últimos estados de funcionamento bons conhecidos de forma rápida e fácil, graças a backups criptografados invioláveis e mecanismos de restauração seguros e protegidos.

Zerto

Em 2021 a HPE concluiu a aquisição da Zerto, uma empresa especializada em soluções de recuperação de desastres, recuperação de ransomware e mobilidade multicloud. Agora parte da HPE, a Zerto oferece proteção e recuperação contínua de dados para aplicativos e dados virtualizados e contentorizados, da borda à nuvem. Com a Zerto, as organizações podem se recuperar em minutos para um estado segundos antes de um ataque, eliminando interrupções demoradas e dispendiosas e perda de dados. A Zerto traz maior disponibilidade com uma sobrecarga administrativa muito menor do que as soluções de proteção de dados legadas. Além disso, o gerenciamento de dados unificado, escalável e automatizado da Zerto torna a carga de trabalho e a mobilidade de dados entre nuvens fácil e direta. Além disso, a Zerto oferece proteção contínua de dados para organizações que empregam uma estratégia de nuvem híbrida e inclui Recuperação de desastres como serviço (DRaaS) com uma rede de mais de 350 provedores de serviços gerenciados. Acesse a página da HPE/Zerto para saber como a sua empresa pode evitar perdas de dados e deixar o tempo de inatividade de aplicativos tão próximo de zero quanto a tecnologia consegue alcançar.

SOLUÇÕES DE SEGURANÇA DA HPE

As ferramentas, tecnologias e soluções de segurança da HPE empregam três abordagens principais em todo o projeto, desenvolvimento, fabricação e manutenção. Elas são melhor descritas da seguinte forma:

- **Segurança centrada em dados:** As medidas de segurança procuram proteger os dados em primeiro lugar, particularmente os dados com qualquer tipo de sensibilidade (informações de identificação pessoal ou PII; contas e senhas; dados financeiros, de saúde ou outros dados protegidos por lei, e assim por diante). Isso está diretamente relacionado à próxima abordagem, que se concentra em quem obtém acesso a sistemas e dados e para quais finalidades.

> **Envolver parceiros experientes (como a HPE e seus parceiros) pode preencher as lacunas de habilidades cibernéticas em seus negócios e mitigar vulnerabilidades.**

- **Segurança zero-trust:** O NIST (National Institute of Standards and Technology) descreve zero trust (ZT) com o epigrama: "Nunca confie; sempre verifique". A ZT se concentra na proteção de dados e serviços, mas também deve incluir todos os ativos (dispositivos, elementos de infraestrutura, aplicativos, além de recursos virtuais e de nuvem) e personas (usuários, aplicativos, serviços e sistemas). Basicamente, a ZT considera que os invasores estão sempre presentes e ativos. Assim, ela não deposita confiança implícita a ninguém e sempre analisa e avalia os riscos aos ativos e funções de negócios. A verificação de identidade para todas as solicitações de acesso é uma estratégia fundamental, assim como a aplicação do "Princípio do Mínimo Privilégio" (também conhecido como PLP), o que significa não permitir mais privilégios do que os necessários para que as personas realizem seus trabalhos.
- **DevSecOps:** Simplificando, esta é uma extensão da ideia de Desenvolvimento e operações, que coloca desenvolvedores (e pessoal de suporte, como testadores, documentadores e treinadores) juntos da equipe de operações (administradores, suporte técnico e técnicos de campo ou solucionadores de problemas) em uma única organização com metas e objetivos compartilhados. O DevSecOPs vai um passo além e integra a equipe de segurança em todo o ciclo de vida de desenvolvimento, para que a segurança seja considerada durante as fases de projeto, construção, teste, manutenção e desativação nas operações de TI de negócios.

ALÉM DAS SOLUÇÕES: AJUDA COM CONSULTORIA ESPECIALIZADA

A HPE Pointnext Services pode ajudar pequenas e médias empresas a auditar, definir e refinar suas estratégias de segurança. A Pointnext oferece assistência especializada na formulação de políticas de segurança e no cumprimento dos requisitos de conformidade para privacidade, confidencialidade e proteção de dados. Ela também pode ajudar empresas com recursos ou conhecimentos limitados a integrar soluções acessíveis

e eficazes para continuidade de negócios e recuperação de desastres. Na verdade, a Pointnext é especializada em ajudar as empresas a preparar planos de segurança para fundamentar projetos e implementações de segurança na realidade (e dentro das restrições orçamentárias). Ela também pode fornecer assistência de ponta a ponta por meio de implantações de teste, piloto e produção. Por fim, a Pointnext pode ajudar as empresas a garantir que a segurança seja integrada em toda a organização: trabalhadores remotos, na borda, no local e em ambientes híbridos e multicloud.

Proteção da cadeia de suprimentos

A HPE opera uma Cadeia de suprimentos confiável (TSC) para atender clientes com requisitos de segurança acima do normal e cenários de uso altamente seguros. Os clientes representativos dessa cadeia de suprimentos incluem organizações e agências do governo e do setor público dos EUA que devem adquirir produtos fabricados nos EUA com garantia verificável do produto. A segurança entra na TSC de duas maneiras importantes. Primeiro, esses produtos incluem recursos de segurança reforçados projetados para torná-los resistentes a adulteração, se não invioláveis. Em segundo lugar, a HPE supervisiona toda a cadeia de suprimentos e aprova todas as peças, observa a montagem e mantém os produtos embalados seguros (e livres de adulteração) até que os clientes aceitem a entrega.

O Project Aurora oferece uma arquitetura de segurança completa com novas soluções integradas e incorporadas de segurança que começam no nível do silício. Saiba como o Project Aurora é acionado na cadeia de suprimentos e estabelece uma cadeia de confiança imutável na infraestrutura, no sistema operacional (OS), na plataforma de software e nas cargas de trabalho sem exigir assinaturas, comprometimento significativo no desempenho ou dependência.

As ferramentas, tecnologias e soluções de segurança da HPE empregam três abordagens principais em todo o projeto, desenvolvimento, fabricação e manutenção.

A HPE e seus parceiros oferecem uma ampla variedade de soluções de segurança cuidadosamente elaboradas para ajudar pequenas e médias empresas a gerenciar riscos, proteger seus sistemas e dados e lidar com o cenário de segurança complexo e proibitivo de hoje. Acesse a página Soluções de TI para pequenas e médias empresas da HPE para conhecer todos os detalhes. Considere ainda que a HPE e seus parceiros também podem oferecer treinamento, consultoria, assistência e serviços para ajudar as empresas menores a permanecerem seguras e protegidas por meio de sua organização de serviços Pointnext.