DELL Technologies

Protegendo endpoints em meio a novas ameaças

Para que os funcionários tenham flexibilidade para ser totalmente produtivos enquanto trabalham remotamente, é essencial que as empresas tenham medidas de segurança de endpoints em vigor para impedir e detectar ameaças, responder ao crescente ambiente de ameaças e, ao mesmo tempo, proporcionar flexibilidade para que os funcionários trabalhem remotamente.

À medida que os líderes de TI examinam o horizonte por indícios do fim da pandemia de COVID-19, muitos estão planejando um novo normal, com um número de funcionários remotos maior que nunca. Embora muitas empresas e seus funcionários vão se beneficiar da maior produtividade e do estilo de trabalho mais flexível, isso terá um preço em termos de proteção. O aumento do trabalho remoto devido à COVID-19 dificultou ainda mais a proteção dos endpoints: 84% dos líderes de TI dizem que proteger uma força de trabalho remota é mais difícil.[1] Uma explicação provável para isso é o aumento de 148% nos ataques de ransomware às organizações globais em meio à pandemia.[2] O que torna essa estatística preocupante é o fato de que os funcionários em home office dependem do e-mail como seu principal meio de comunicação empresarial, o que resultou em um aumento de 350% nos ataques de phishing.[3]

Tendências contínuas de segurança cibernética

A mudança repentina para o trabalho remoto ocorre em um cenário de muitas preocupações perturbadoras com a segurança cibernética, que estão sobrecarregando o conhecimento especializado dos profissionais dessa área. Dentre elas:

1. Ataques em nível de BIOS — vulnerabilidades exploradas no hardware ou no chip. Quando o BIOS é comprometido, o invasor geralmente permanece oculto enquanto o dispositivo tem acesso credenciado à rede e aos dados. 63% das empresas sofreram um comprometimento ou violação de dados como resultado desses ataques.[4]
2. Ameaças avançadas persistentes (APTs) — ameaças sofisticadas que, muitas vezes, aguardam silenciosamente à medida que coletam informações comportamentais antes de extrair dados valiosos. Por muito tempo (108 dias, em média[5]), as vítimas podem não perceber que ocorreu um ataque silencioso.
3. Malware sem arquivos e baseado em arquivos
   - Malware baseado em arquivos — geralmente, são tipos de arquivos com extensões familiares, como .DOCX e .PDF — o tipo de arquivo de que os funcionários precisam para trabalhar. Quando um usuário abre o arquivo, o código mal-intencionado integrado é executado.
   - Malware sem arquivos — geralmente, um programa legítimo que infecta um computador. Quando o usuário inicia esse programa a partir do e-mail, o malware sem arquivos infecta o computador e, possivelmente, a rede, contornando muitas tecnologias de segurança com sucesso.
4. Ataques de estados-nação — geralmente, são provenientes da China, da Coreia do Norte, da Rússia e do Irã. Com o conhecimento tecnológico especializado e o apoio financeiro desses estados-nação, muitas vezes, os ataques são sofisticados e muito prejudiciais. No entanto, muitos deles exploram sistemas que não têm as atualizações e os patches mais recentes. A unidade CISA do FBI envia aconselhamentos regularmente sobre isso.

A mudança repentina para o trabalho remoto ocorre em um cenário de muitas preocupações perturbadoras com a segurança cibernética, que estão sobrecarregando o conhecimento especializado dos profissionais dessa área.

1. "The State of DLP 2020", Tessian.
2. Blog VMware Carbon Black, Patrick Upatham e Jim Treinen, 15 de abril de 2020.
3. Relatório do Google, conforme citado em PCMAG.com, 30 de março de 2020.
4. "Match Present-Day Security Threats with BIOS-Level Control", artigo de liderança de ideias da Forrester Consulting encomendado pela Dell, junho de 2019.
5. Pesquisa 2018 U.S. State of Cybercrime.

5. Ataques na nuvem — aumentam à medida que os aplicativos colaborativos e de produtividade na nuvem substituem os aplicativos de desktop. Como uma empresa média usa mais de 2.400 serviços em nuvem, 93% das organizações estão moderadamente ou extremamente preocupadas com a segurança da nuvem.[6] A proteção deve incluir prevenção contra perda de dados (DLP) e proteção contra ameaças na nuvem. Além disso, a autenticação do usuário deve ser protegida contra falsificação, e os dados enviados e recebidos da nuvem devem ser criptografados.
6. Normas de conformidade — visam a proteger informações de identificação pessoal (PII). Para impedir que as PII caiam nas mãos erradas e, em última análise, sejam usadas para roubo de identidade, alguns setores adotaram normas rígidas que envolvem duras penalidades. Essas normas incluem a HIPAA na área da saúde, PCI-DSS em serviços financeiros e varejo e GDPR para empresas que fazem negócios com cidadãos europeus.
7. Riscos devastadores — resultantes da previsão para 2021 de US$ 6 trilhões em prejuízos gerados por crimes cibernéticos, o que representa um aumento de US$ 3 trilhões em relação a 2015. Os prejuízos são causados por dano e destruição de dados, roubo de fundos, perda de produtividade, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, disrupção após os ataques, danos à reputação e muito mais, de acordo com a Cybersecurity Ventures.[7]

Repensando a segurança de endpoints

Segurança de endpoints: parte da segurança empresarial
Diante de uma população de funcionários remotos maior do que nunca, muitos dos quais devem lidar com dados confidenciais para trabalhar, os líderes de TI devem avaliar o estado atual da segurança de endpoints de suas organizações. Mas, em vez de analisar a segurança de endpoints por si só, eles devem considerá-la como parte integrante da segurança empresarial para implementar a proteção a fundo — e devem ir além dos endpoints para incluir armazenamento, redes e serviços na nuvem. Uma abordagem holística para a criação de "dispositivos confiáveis" na empresa deve considerar estes fatores:

Segurança integrada
Em vez de depender exclusivamente do software para proteger os endpoints, uma abordagem abrangente exige o uso de dispositivos confiáveis: dispositivos de computação de usuário final que implementam a segurança nos próprios dispositivos. Esses dispositivos protegem as PII e desempenham um papel importante na conformidade com normas, em caso de perda ou roubo de dispositivos. Os dispositivos de usuário final também devem incluir uma tecnologia de privacidade para telas, que limita a capacidade dos colegas de trabalho e dos visitantes do escritório de visualizar informações confidenciais na tela de um computador.

Os líderes de TI devem considerar a segurança de endpoints como parte integrante da segurança empresarial.

6. Relatórios de segurança na nuvem por profissionais de segurança cibernética, 2018, 2019.
7. Cybersecurity Ventures, 2020.

Proteção acima e abaixo do So

Acima do SO. A TI precisa de visibilidade, monitoramento e segurança de dados, além de prevenção, detecção e correção de ameaças. A criptografia no dispositivo também é muito importante para atender aos requisitos de conformidade; no entanto, ela não deve retardar o desempenho nem diminuir a produtividade do usuário.

Abaixo do SO. A TI precisa de proteção do BIOS e autenticação de chips, devido à frequência de ataques ao firmware e ao hardware. Um BIOS comprometido pode oferecer aos invasores o acesso a todos os dados de um endpoint, inclusive credenciais, permitindo que eles se movam na rede de uma organização e ataquem a infraestrutura de TI mais ampla.

Inteligência artificial e aprendizagem automática

Com os ataques atuais cada vez mais sofisticados, o uso de inteligência artificial e aprendizado de máquina para a detecção e correção é essencial à proteção de endpoints. Observando padrões comportamentais, os algoritmos de IA e ML podem detectar atividades incomuns que podem indicar violações e impedi-las.

Cadeia de suprimentos segura

No processo de produção, agentes mal-intencionados podem introduzir componentes comprometidos para permitir um ataque de backdoor. Depois de integrados a um produto acabado, esses componentes podem proporcionar uma violação que pode ser extremamente prejudicial e difícil de detectar. Portanto, é essencial que os fornecedores e fabricantes implementem medidas rigorosas de segurança em pontos críticos da cadeia de suprimentos.

Dell Trusted Devices

A Dell agrega segurança aos PCs com estas tecnologias:

SafeBIOS com indicadores de ataque (IoA) ao BIOS — oferece visibilidade sobre as alterações do BIOS para impedir adulterações. A Dell mantém uma imagem protegida fora do host para verificar a integridade do BIOS. Agora, o SafeBIOS é integrado ao VMware Carbon Black Audit and Remediation, o que aumenta a visibilidade dos ataques por meio de relatórios automatizados e permite o acesso remoto para corrigir a corrupção do BIOS.

SafeID — oferece autenticação baseada em chip. As credenciais do usuário final são verificadas com um chip dedicado de segurança, em vez de depender de software, que é menos seguro.

SafeScreen — protege as telas que podem expor informações confidenciais a colegas de trabalho, visitantes, funcionários de manutenção ou outras pessoas não autorizadas do escritório.

SafeGuard and Response. Alimentado pelas tecnologias VMware Carbon Black e Secureworks, o portfólio da Dell inclui:

VMware Carbon Black — uma plataforma de proteção de endpoints nativa na nuvem que combina a prevenção comportamental e o fortalecimento inteligente do sistema necessários para conter as novas ameaças, usando um só agente leve e um console fácil de usar.

Os dispositivos confiáveis protegem as PII e desempenham um papel importante na conformidade com normas, em caso de perda ou roubo de dispositivos.

Secureworks Managed Services — coleta e correlaciona a telemetria da nuvem, da rede e dos endpoints para identificar ameaças em toda a empresa. Oferecendo uma resposta a incidentes líder do setor, os Secureworks Managed Services são integrados à plataforma VMware Carbon Black e muitas outras plataformas.

SafeData. A colaboração, característica das organizações de sucesso, assume uma maior importância na era do trabalho remoto intensificado. A colaboração da atual força de trabalho exige segurança de dados no dispositivo e na nuvem, sem retardar o usuário final. A Dell tem parcerias com a Netskope e a Absolute para entregar uma segurança abrangente para endpoints.

Netskope. Adotando uma abordagem concentrada em dados, a tecnologia Netskope protege os dados criados e expostos na nuvem. Ao oferecer à TI visibilidade em tempo real, acesso à nuvem, monitoramento e prevenção contra perda de dados, a Netskope redefine a segurança da nuvem, da rede e dos dados. As equipes são capacitadas com o equilíbrio certo entre proteção e velocidade, o que permite que elas protejam a jornada de transformação digital da organização.

Absolute. A Dell integra a tecnologia Absolute ao firmware de todos os dispositivos, oferecendo aos endpoints um link de autocorreção para o painel de indicadores da Absolute na nuvem. Como resultado, os gerentes podem rastrear, gerenciar e proteger os endpoints e os dados que eles contêm, mesmo quando estiverem fora da rede. A tecnologia Absolute:

- Localiza e gerencia dispositivos.
- Oferece persistência da VPN e do software de segurança.
- Implementa uma solução isolada para permitir a recuperação de ataques
- Inclui soluções de proteção de dados em várias nuvens que podem ser definidas por software ou baseadas em equipamentos.

A colaboração da atual força de trabalho exige segurança de dados no dispositivo e na nuvem, sem retardar o usuário final.

Conclusão

O aumento do trabalho remoto devido à pandemia de COVID-19 aumenta os perigos em um ambiente de segurança cibernética já repleto de ameaças. Por isso, é necessário adotar uma nova abordagem holística para a proteção de endpoints. Para repensar a proteção de endpoints, é preciso começar com dispositivos confiáveis que estejam protegidos acima e abaixo do SO. Essa estratégia também vai além dos próprios endpoints para permitir uma visão empresarial da segurança cibernética que inclua servidores, redes, serviços em nuvem e conformidade com normas. O portfólio Dispositivos Confiáveis da Dell incorpora esse tipo de abordagem abrangente. A proteção de endpoints da Dell abrange toda a empresa para incluir soluções de proteção de dados em várias nuvens, que possam ser entregues como soluções definidas por software e/ou baseadas em equipamentos. Acima de tudo, os Dispositivos Confiáveis da Dell permitem que os usuários permaneçam altamente produtivos, frustrando ataques cada vez mais sofisticados no novo paradigma de trabalho remoto.

Para obter mais informações, acesse:
https://www.delltechnologies.com/pt-br/endpoint-security/index.htm