Navegando pela Nova Empresa Distribuída

Os primeiros dias da pandemia de COVID-19 foram como um abalo sísmico para TI e os Gerentes de Segurança.. Quase da noite para o dia, governos e outras entidades instituíram confinamentos para tentar conter a propagação do vírus - e a TI, de repente, teve de apoiar uma nova força de trabalho distribuída.

Três anos depois, a COVID-19 continua circulando, apesar da grande diminuição da incidência de casos.[1] No entanto, a tendência do trabalho remoto permanece forte, em razão, no mínimo em parte, à demanda do funcionário.[2] Agora que a força de trabalho híbrida ou distribuída se tornou o novo normal, é imperativo garantir a confiabilidade digital, segurança e integridade dos usuários, dispositivos e ativos sejam de qualidade, não importante onde eles residam fisicamente.

Assumindo o Controle dos Ativos

Os dias de redes altamente controladas, servidores e terminais de usuários acabaram. Agora é comum para servidores, aplicações e outros ativos abrigados ou possuídos separadamente - e, no mínimo, de alguma forma fora do alto controle da TI. Considerando a migração e a penetração da TI invisível entre os usuários ou departamentos fora do domínio da TI,[3] é essencial implementar a descoberta de ativos como parte do processo de gerenciamento de ativos..

A descoberta de ativos é um exercício fundamental para identificar todos os ativos que conectam a rede da empresa e determinar a importância e criticidade de cada um. O processo deve ser contínuo, automático e reforçado através de atualizações manuais quando necessário. Uma ampla variedade de ferramentas de descoberta de ativos estão disponíveis, desde softwares gratuitos a softwares e serviços licenciados de classe empresarial.[4]

Uma Abordagem Baseada em Risco

Possuir um inventário de ativos preciso, prepara para a TI para identificar os recursos críticos que precisam ser protegidos contra atos maliciosos e uso indevido. Dependendo do ambiente e recursos de pessoas, uma abordagem baseada em risco é requerida para proteger os ativos de alto valor ou possuem alto risco evidenciado em termos de comportamento.

Estes podem incluir ativos de elevado número de anormalidades, indicadores gerais de comprometimamento (indicators of compromise - IoCs), ou outros fatores que os classifiquem especialmetne como vulneráveis a ataques. Fazer esta determinação geralmente está além do escopo dos sistemas de gerenciamento de ativos, assim como decifrar a interconectividade entre os ativos. Para estes casos de uso, um sistema estendido de detecção e resposta (extended detection and response - XDR), pode ser benéfico devido a sua habilidade de reunir e contextualizar dados de diversas fontes, fornecendo uma visibilidade e mapeamento detalhados.

Exigências do Terminal

Em uma força de trabalho distribuída ou híbrida, deve-se considerar especialmente o cliente, os dispositivos móveis e os equipamentos traga seu próprio dispositivo (bring-your-own-device - BYOD). O mais importante é se o acesso à rede e aos recursos será restribo a dispositivos de propriedade da empresa ou se também será permitido para terminais do usuário. Restrições de dispositivo, geralmente baseado em sistema operacional (operating system - OS),

TIMOTHY LIU

É cofundador e diretor de tecnologia da Hillstone Networks, uma provedora líder de soluções de proteção de infraestrutura. Ele tem mais de 25 anos de experiência nos setores de tecnologia e segurança trabalhando com empresas Fortune 500 e centros de dados para defender-se proativamente contra ataques cibernéticos em nível global.

O suporte integral da força de trabalho distribuída exige também uma mudança fundamental do controle de acesso a rede baseado em endereço de IP para identificar NAC baseado em identidade.

ou endereço de controle de acesso à mídia (media acess control - MAC), é frequentemente através de soluções de segurança de perímetro. Por exemplo, firewall de próxima geração permitem a TI exerça rígido controle sobre quais dispositivos podem acessar a rede e seus ativos.

Para todos so terminais, independente da propriedade ou localização física, verificação de segurança é fundamental para garantir a integridade do dispositivo e confiabilidade digital. Tipicamente, isso é executado por um agende de terminal como cliente Secure Sockets Layer Virtual Private Network (SSL VPN), que pode suportar sistemas operacionais de múltiplos dispositivos (operating systems - OSs) e verificar versões OS, proteção contra vírus e outras condições.

Outra consideração é o potencial de perda ou roubo de um terminal pessoal ou de propriedade da empresa que pode expor informações corporativas confidenciais. Rastreamento de dispositivos, a capacidade de limpar dados no final da sessão ou outro critério, criptografia e múltiplo fator de autenticação (multifactor authentication - MFA) são importantes.

De Controle de Acesso de Rede Baseado em IP a Controle Baseado em ID

Apoiar integralmente a força de trabalho distribuída exige também uma mudança fundamental do controle de acesso a redes baseadas em endereço (network access control - NAC) de Protocolo de Internet (Internet Protocol -IP). A NAC baseada em IP, usando diretório ativo ou mecanismos similares, vem sendo utilizada para apoiar dispositivos instalados on-premises. Esta abordagem amplia a segurança permitindo que apenas dispositivos conectados a redes específicas (endereços de IP) acessem os dados sensíveis e recursos da empresa.

No entanto, em ambientes distribuídos, uma NAc centralizada pode se tornar um ponto único de falha. Por exemplo, conexões de rede não confiáveis podem resultar em aprovações irregulares de acesso a rede para usuários remotos. Além disso, trabalhadores distribuídos e remotos são mais móveis do que suas contrapartes frequentando escritórios. Um trabalhador remoto pode fazer login através de um ponto de acesso WiFi público, uma rede de telefonia móvel compartilhada ou algum outro ponto de acesso-tornando um esquema NAC baseado em IP difícil ou impossível de reforçar.

Como resultado, muitas empresas estão mudando para Identidade como Serviço (Identity as a Service – IdaaS) baseado em nuvem com alternativa.[5] IDaaS é um serviço de gestão de identidade distribuído e gestão de acesso (IAM)[6] com NAC incorporado como coponente. O modelo IDaaS oferece a escalabilidade, adaptabilidade e agilidade da nuvem, redução da sobrecarga de gerenciamento e gastos de capital, além de ampla distribuição geográfica e, em muitos casos, integração mais fácil com outros recursos da nuvem, como Software como Serviço (Software as a Service - SaaS).

O IDaasS também pode oferecer serviços avançados de acesso seguro, como MFA adaptativo, logon único na rede - e recursos empresariais baseados em nuvem, e até mesmo portais de auto atendimento que permitem aos usuários solicitar seus acessos e atualizar suas informações. No entanto, o IDaaS não é isento de inconvenientes ou riscos. O provedor pode limitar as permissões incluídas na oferta de IDaaS, e as violações são possibilidade real, conforme evidenciado pelo recente ataque de ransonware Okta.[7]

Considerações da Nuvem

Com NAC tradicional e IAM baseado em nuvem, a implementação da nuvem em geral se tornou uma parte importante - quase intrínseca - de apoiar a força de trabalho distribuída. 94% de todas as empresas atualmente utilizam serviços em nuvem, e 48% das empresas armazenam informações restrivas e demais informações relevantes na nuvem.[8]

Apesar da localização de aplicativos e recursos baseados em rede tradicionalmente funcionarem bem para funcionários instalados no local de trabalho, o novo modelo de força de trabalho distribuído exige que os recursos estejam igualmente disponíveis para trabalhadores remotos e móveis. Os gerentes de TI precisarão cada vez mais facilitar o movimento de aplicativos internos (apps) para a nuvem, incluindo arquiteturas em nuvem híbrida e pública, para melhor apoiar os trabalhadores, independentemente da localização.

No entanto, as considerações sobre segurança e, por extensão, as questões de confiabilidade digital para os usuários que acessam aplicativos e bancos de dados na nuvem pública são muito diferentes das associadas a recursos hospedados localmente. Por exemplo, os provedores de nuvem geralmente operam em um modelo de responsabilidade de segurança compartilhado o que torna o provedor responsável por proteger a infraestrutura, mas atribui ao cliente a responsabilidade pela segurança e integridade dos seus próprios aplicativos e dados hospedados.

Adicionalmente, os aplicativos nativos de nuvem e seus variantes continuam a ganhar impulso para extrema flexibilidade, adaptabilidade e utilizada que eles oferecem.[9] Esses aplicativos existem exclusivamente na nuvem e

exigem considerações adicionais relacionadas à segurança cibernética e confiabilidade digital.

Existem muitos produtos de segurança de pontos disponíveis para elementos em nuvem; no entatno, eles fornecem uma janela relativamente estreita para ameaças potenciais, especialmente se a infraestrutura da nuvem for especialmente grande ou abranja múltiplos provedores de serviços em nuvem. Assim, muitas organizações estão investigando as plataformas de proteção de carga de trabalho em nuvem (cloud workload protection platforms - CWPPs), que podem abranger ambientes multinuvem, contêiners, micro serviços, aplicativos nativos em nuvem, máquinas virtuais (virtual machines - VMs) e outros recursos.

Diferentemente dos produtos de segurança de pontos díspares e desconexos, as CWPPs são projetadas para abranger toda a pilha da nuvem - de DevOps a gestão de imagem e tempo de execução. Na etapa de DevOps, a CWPPs fornecem análise de código, encapsulamento e varredura de imagem para ajudar a garantir a integridade e segurança de código e embalagem. Gerenciamento de imagem abrange mais varredura de imagens para proteger contra falhas e ameaças e controle de acesso do usuário para proteger o armazenamento de imagens.

Em tempo de execução, as defesas são geralmente divididas em duas categorias principais: segurança da camada de plataforma e segurança do tempo de execução. A primeira normalmente inclui segurança para a arquitetura, rede, hospedagem, kernel e Docker daemon; linha de base de conformidade; controle de acesso; criptografia e gerenciamento de segurança. A segurança de tempo de execução do contêiner geralmente cobre L7 e isolamento de contêiner, detecção de ameaça, varredura de vulnerabilidades e gestão de processos.

Recursos de CWPP

Como a tecnologia CWPP é relativamente nova, ela normalmente inclui recursos de destaque que são especialmente pertinentes para ambientes multinuvem e de contêiner. Por exemplo, as arquiteturas de contêiner normalmente não são vinculadas aos endereços de IP, mas migram e mudam instantaneamente, conforme necessário. Como resultado, a gestão de ativos do contêiner CWPP precisa conectar com o sistema de orquestração do contêiner, como Kubernetes, para sincronizar os atributos de diversos ativos.

Esse recurso também atua na visualização do tráfego de ativos, um componente crítico da segurança cibernética. Certos sistemas de orquestração não possuem capacidade de segmentar contêiners ou grupos para prevenir acesso ilegal ou malicioso. Acessando o mecanismo de tráfego do componente de orquestração, a CWPP pode detectar e exibir tráfego entre contêiners, redes externas e demais ativos. Isso permite aos administradores visualizar rapidamente as interações dos ativos do contêiner, controlar e detectar qualquer tentativa de acesso ilegal.

Visualização precisa também permite que uma CWPP reforce a micro segmentação de cargas de trabalho em nuvem para evitar a rápida propagação de malware entre ativos e reduzir acessos ilegais. A maioria dos sistemas de orquestração fornece algum tipo de mecanismo para essa função, mas são tipicamente trabalhosos e carecem de recursos de registro. A CWPP, ao contrário, oferece micro segmentação através de uma interface gráfica de usuário (graphical user interface - GUI) para permitir fácil controle e visualização com apenas alguns cliques e registro completo para perícia.

Como a tecnologia CWPP é relativamente nova, ela normalmente inclui recursos de destaque que são especialmente pertinentes para ambientes multinuvem e de contêiner.

Estabelecendo Confiabilidade Digital

Nenhuma conversa sobre confiança digital seria completa sem endereçar os desafios de garantir acesso para funcionários e outros, independentemente de sua localização física. Quando a pandemia da COVID-19 e os confinamentos associados chegaram, a maioria das equipes de TI buscaram uma tecnologia que já estava em vigor para acesso remoto seguro: Secure Sockets Layer virtual private network (SSL VPN) - rede virtual privada Secure Sockets Layer

No entanto, a instalação da SSL VPN em escala para suportar centenas ou milhares de trabalhadores dispersos trouxe rapidamente em foco certas limitações e outros problemas. Por exemplo, SSL VPNs de classe empresarial são geralmente licenciados por usuário ou por capacidade. Expandir para suportar usuários remotos adicionais pode encarecer rapidamente em termos de licenças, custos adicionais de hardware e tempo de pessoal de TI para administrar as permissões e os dispositivos do usuário.

Adicionalmente, algumas VPNs autenticarão os usuários uma única vez - no inicio da sessão - e depois darão acesso a todos os ativos e recursos aos quais o usuário estiver autorizado. O risco de segurança então surgirá se as credenciais do usuário forem roubadas por um hacker ou se o próprio dispositivo do usuário for hackeado. Finalmente, as SSL VPNs vêm exibindo múltiplas vulnerabilidades nos últimos anos, na medida em que a US National Security

QUER SABER MAIS?

- Leia *Zero Trust: How to Beat Adversaries at Their Own Game. www.isaca.org/zero-trust*
- Saiba mais, discuta e colabore com a gestão de riscos nos fóruns on-line da ISACA. *https://engage.isaca.org/onlineforums*

Agency (NSA) emitiu uma consultoria de segurança cibernética em 2019.[10]

Essas são algumas da principais razões porque muitas organizações estão buscando acesso a rede de confiança zero (zero-trust network access - ZTNA), que dita, em resumo, nunca confie, sempre verifique. Precursores da definição atual circula entre os pesquisadores desde meados dos anos 1990, mas isso foi formalmente codificado na Publicação especial 800 -207 do US National Institute of Standards and Technology (NIST) *Zero Trust Architecture* em 2020.[11] O modelo confiança zero elimina a confiança implícita de usuários e dispositivos, ao mesmo tempo concedendo apenas os privilégios mínimos possíveis. Autenticação é contínua, portanto, se for alguma alteração na postura de segurança do dispositivo ou do usuário for detectada, os direitos de acesso podem ser revogados.

É importante observar que a ZTNA deixa o foco centrado em rede tradicional para abraçar o modelo usuário-para-aplicativo. Isso permite que dispositivos e usuários sejam avaliados de forma abrangente quanto à identidade, postura e contexto das solicitações de acesso. Expande também a segurança além do perímetro da rede para abranger todos e quaisquer recursos conectados à rede - sejam eles baseados em nuvem, remotos, virtuais ou qualquer outra permutação.

Talvez, ainda mais importante, a ZTNA não exige uma substituição completa (e dispendiosa) das atuais infraestruturas de segurança remota. Em vez disso, pode coincidir com as arquiteturas SSL VPN existentes, aumentando e expandindo os serviços de segurança enquanto é implantado gradualmente para atender diretamente outros usuários e grupos.

> A ZTNA não exige uma substituição completa (e dispendiosa) de infraestruturas de segurança de acesso remoto atuais.

Conclusão

Para muitas empresas, rotinas de trabalho mudam drasticamente nos primeiros dias da pandemia do COVID-19, e é improvável que volter ao que eram. Assim, é improvável que estabelecer um estado de confiança digital na nova força de trabalho distribuída seja um processo único. Em vez disso, é muito mais provável que seja um processo incremental que sobrepõe novas técnicas e tecnologias nas infraestruturas atuais permitindo-lhes evoluir em geral para um nível novo e mais elevado de confiança digital e segurança. Além disso, as experiências coletivas das equipes de TI e de segurança no apoio da empresa distribuída provavelmente apontarão para novos modelos de estabelecimento de confiança digital.

Notas finais

1 World Health Organization (WHO), "WHO Coronavirus (COVID-19) Dashboard," *https://covid19.who.int/*

2 Remoters, "Remote Work Trends to Look for in 2023," *https://remoters.net/remote-work-trends-future-insights/*

3 Walters, M.; "Four Practical Steps to Eliminate Shadow IT Permanently," *Forbes*, 25 February 2022, *https://www.forbes.com/sites/forbestechcouncil/2022/02/25/four-practical-steps-to-eliminate-shadow-it-permanently/*

4 Creamer, L.; "The Best IT Asset Management Software," *PC Magazine*, 13 July 2019, *https://www.pcmag.com/picks/the-best-it-asset-management-software*

5 Hughes, C.; "IDaaS explicado: How It Compares to IAM," *CSO*, 23 May 2022, *https://www.csoonline.com/article/3660554/idaas-explained-how-it-compares-to-iam.html*

6 National Institute for Standards and Technology (NIST), "Identity and Access Management," USA, *https://www.nist.gov/identity-access-management*

7 Carey, S.; "LAPSUS$ Ransomware Group Claims Okta Breach," *CSO*, 22 March 2022, *https://www.csoonline.com/article/3654273/lapsus-ransomware-group-claims-okta-breach.html*

8 Sumina, V.; "Twenty-Six Cloud Computing Statistics, Facts and Trends for 2023," Cloudwards, 7 June 2022, *https://www.cloudwards.net/cloud-computing-statistics/*

9 Mia-Platform Team; "Top Four Cloud Native Trends in 2022 Shaping the Future of Business," Cloud Native Computing Foundation, 5 January 2022, *https://www.cncf.io/blog/2022/01/05/top-4-cloud-native-trends-in-2022-shaping-the-future-of-business/*

10 National Security Agency, "Mitigating Recent VPN Vulnerabilities," USA, October 2019, *https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF*

11 Rose, S.; O. Borchert; S. Mitchell; S. Connelly; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 *Zero Trust Architecture*, USA, 2020, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf*