Segurança Cibernética para as Empresas

Folheto

Alcatel·Lucent Enterprise

Visão geral

Não é de hoje que a segurança cibernética é uma prioridade para as empresas. No entanto, as exigências de segurança cibernética estão mudando devido à transformação digital que está ocorrendo. A transformação digital significa que as organizações usam mais dispositivos conectados e móveis em suas redes, enquanto os funcionários estão acessando cada vez mais aplicativos e dados externos à rede.

À medida que a mudança se acelera, os velhos métodos de segurança de rede já não conseguem acompanhar o ritmo. Este documento compartilha percepções sobre as forças que estão mudando os requisitos atuais de segurança cibernética corporativa e recomenda estratégias que as empresas podem adotar e tecnologias a serem implantadas para manter os dados e sistemas seguros na era da transformação digital.

A solução de segurança cibernética da Alcatel-Lucent Enterprise atende às demandas de uma empresa transformada digitalmente. Com uma abordagem multifacetada à segurança cibernética, as empresas podem oferecer acesso baseado em políticas aos dispositivos conectados, dados seguros e aplicativos de software em todo o ecossistema corporativo.

Novos desafios

A natureza das ameaças de segurança cibernética está mudando. Os hackers estão usando inteligência artificial (IA) e machine learning (ML) para criar ataques mais sofisticados e automatizados. Novas técnicas de engenharia social permitem aos criminosos conectar informações encontradas nas mídias sociais ou dos dados mantidos pelas organizações para criar perfis de indivíduos.

A transformação digital nas empresas também está impactando os requisitos de segurança cibernética, resultando em maior complexidade, maior uso de dispositivos conectados, desaparecimento de limites, e tudo isso a um ritmo acelerado.

Mais dispositivos, mais complexidade

As empresas estão adotando novas tecnologias, incluindo nuvem, mobilidade, IoT, Big Data, e análises avançadas. Estas novas soluções introduzem um novo nível de complexidade que requer uma nova forma de olhar para a segurança. Além disso, conforme o número de dispositivos conectados aumenta, também aumentam as vulnerabilidades e oportunidades para violações.

Por exemplo, a primeira geração de dispositivos conectados não necessitava de senhas. Com os dispositivos conectados à rede, os hackers poderiam usá-los como um gateway para a rede. Hoje em dia, recursos de segurança como senhas hardcoded são muitas vezes mandados para dispositivos, no entanto, as violações permanecem inevitáveis e quando elas ocorrem, os hackers ainda podem ganhar acesso à rede.

O perímetro está desaparecendo

A maioria das organizações tem, há muito tempo, demarcado claramente o limite entre usuários e recursos dentro e fora da rede. Contudo, à medida que as organizações abraçam a transformação digital, tornam-se mais abertas a trocas com um ecossistema mais amplo, incluindo outros parceiros e provedores em um ambiente integrado colaborativo. Os usuários já não acessam simplesmente os recursos de dentro do perímetro da rede – eles podem estar em qualquer lugar. Informações podem ser trocadas com contatos em uma rede diferente. Os recursos de TI também já não estão confinados ao perímetro da empresa. Eles podem estar no local ou na nuvem, e conectados através de APIs. As empresas precisam de formas modernas de proteger os recursos quando o perímetro já não existe.

Macro e micro-segmentação, em um mundo de confiança zero

Existem dois tipos de segmentação, macro e micro. Na macro-segmentação, a rede física é dividida em diferentes segmentos lógicos. Todas as empresas utilizam a segmentação, mas nem sempre por razões de segurança. Muitas vezes, a macro-segmentação é usada para fins administrativos, organizacionais ou de escalabilidade. Esses segmentos podem ser uma VLAN, uma combinação de VLAN + VRF, também pode ser uma VPN quando se fala de Shortest Path Bridging, MPLS, ou mesmo túneis VXLAN ou GRE. O tráfego entre usuários ou dispositivos em diferentes segmentos é controlado por um firewall físico. Se dois dispositivos forem mapeados para VLANs diferentes e puderem se comunicar sem passar por um firewall, eles estarão no mesmo macro-segmento. Por exemplo, câmeras e fechaduras podem ficar sob o controle do grupo de segurança de acesso, enquanto os termostatos podem ficar sob o controle do grupo de manutenção do edifício.

A micro-segmentação leva as coisas um passo adiante. Nem todos os usuários são iguais e nem todos os usuários têm uma necessidade legítima de acessar todos os recursos. O mesmo perfil que mapeia usuários para um segmento também inclui um conjunto de políticas que adicionam controle granular sobre privilégios de usuário/dispositivo que são diferentes para funções diferentes, como RH ou Finanças. Isso é conhecido como 'acesso baseado em função' e está diretamente relacionado ao 'princípio de privilégios mínimos'. E assim, embora as câmeras e as fechaduras estejam no mesmo segmento, elas não precisam usar os mesmos recursos. A câmera precisa se comunicar com o gravador de vídeo e a fechadura da porta com seu servidor. Não há necessidade de uma câmera se comunicar com a fechadura, da mesma forma que não há necessidade de que uma fechadura se comunique com outra fechadura. Essas permissões granulares são implementadas por meio de políticas que fazem parte do perfil e são aplicadas dinamicamente ao dispositivo após a autenticação.

A questão é: realmente precisamos de ambos? O desafio de ter uma abordagem apenas de macro-segmentação é que o firewall se torna um gargalo, porque todas as VLANs precisam ser encerradas no firewall e, em seguida, são criados problemas de desempenho. Como alternativa, mais firewalls podem ser implantados na camada de distribuição. No entanto, isso seria muito caro e ainda não é bom do ponto de vista do desempenho. Além disso, ter mais firewalls significa que há vários pontos de aplicação de políticas e vários locais para manter as políticas atualizadas.

A micro-segmentação por si só também pode ser problemática. Se a única imposição de política for feita por meio de políticas de Controle de Acesso à Rede (NAC), as listas de políticas se tornarão longas e complexas e poderão esgotar os limites de capacidade do dispositivo. Um equilíbrio entre esses dois tipos de segmentação permite que o firewall controle o tráfego entre diferentes segmentos (vertical) e as políticas NAC controlem o tráfego dentro de um determinado segmento (lateral). Ao combinar a macro e a micro-segmentação, as ameaças à segurança que se propagam de um segmento de segurança para outro podem ser implementadas, assim como aquelas que se movem lateralmente no mesmo segmento.

Em termos de uma abordagem de confiança zero para a segurança da rede, o princípio orientador é «agir como se os invasores já estivessem presentes». Isso significa autenticar todas as conexões. Nenhum ativo e nenhum usuário é inerentemente confiável. Quer estejam no local ou fora dele, eles passam pelos mesmos controles. Não existe uma confiança pré-estabelecida nos usuários internos. Todo acesso é autenticado.

Se considerarmos uma abordagem tradicional de segurança, onde a rede era vista como uma fortaleza construída em torno da empresa. A fortaleza representa o firewall, de forma que qualquer coisa externa não seja confiável e seja examinada, enquanto qualquer coisa interna seja implicitamente confiável e permitida. Entretanto, a micro-segmentação, especificamente a micro-segmentação definida por software, leva isso um passo adiante. Além da fortaleza, e da segurança ao redor do edifício, há também guardas de segurança que requerem autenticação. Este limite de confiança é difuso, é distribuído e móvel. Não está vinculado a um local específico, porta de switch ou VLAN. Depende da identidade, do dispositivo, da situação e da hora do dia. É definido por software e ajustado em tempo real. A chave para essa abordagem é que os componentes são gerenciados e devem ser capazes de reagir e reconfigurar-se conforme necessário para responder a ameaças ou mudanças no fluxo de trabalho.

Uma solução para a empresa em evolução

A Alcatel-Lucent Enterprise oferece uma abordagem multifacetada à segurança cibernética corporativa, que fornece segurança em profundidade para dispositivos e aplicativos conectados por meio de várias camadas de proteção.

Conectividade flexível

Nossa abordagem começa com uma rede autônoma flexível, que torna rápido e fácil configurar políticas de rede e segurança cibernética para o vasto número de usuários, dispositivos e aplicativos conectados, que alimentam a transformação digital.

No passado, a TI era uma operação de problema/correção. A TI instalava novos equipamentos, colocava em funcionamento e gerenciava a rede usando processos manuais tediosos. A Alcatel-Lucent Enterprise Digital Age Networking oferece uma rede inteligente e automatizada que facilita a conexão de usuários e dispositivos a seus aplicativos específicos de maneira segura. Construído utilizando a tecnologia ALE Intelligent Fabric (iFab), a Digital Age Networking combina o iFab com o padrão do setor, Shortest Path Bridging (SPB). Juntas, essas tecnologias simplificam a criação e configuração de redes, permitindo o roteamento rápido de vários caminhos e a agregação de links para combinar várias conexões de rede em paralelo para aumentar a taxa de transferência e fornecer redundância.

Com a abordagem da ALE, a TI define os serviços de rede, arquitetura, políticas de acesso e contêineres, e a rede se constrói automaticamente. Uma vez que a rede é arquitetada, se algo é movido, alterado ou adicionado, a rede faz os ajustes necessários de forma automática e indetectável. Por exemplo, se um switch estiver fora de serviço, a rede irá se redirecionar automaticamente em torno desse switch.

Usando uma rede autônoma, as empresas se beneficiam da automação que reduz os erros de configuração manual e ajuda a acompanhar o ritmo acelerado das mudanças em suas organizações. Como a automação elimina o trabalho manual, a TI se torna mais um motor de negócios.

Controle de acesso por meio de políticas inteligentes e automatizadas

As empresas podem usar a Digital Age Networking para definir as regras e as políticas de acesso dos usuários, que gerenciam quais aplicativos e dispositivos os usuários podem acessar – e seguir os usuários onde eles forem. Por exemplo, podem estabelecer políticas que permitem acessar:

- Sistemas específicos
- Serviços de internet
- Outros parceiros em casos de serviços por contrato

A ALE também oferece serviços baseados em localização, tais como navegação em ambientes fechados, rastreamento de ativos e pessoas que permitem às organizações estabelecer políticas que levam em conta a localização do usuário.

Os recursos de Gerenciamento Unificado de Políticas de Acesso (UPAM) aplicam as políticas automaticamente toda vez que um usuário se conecta, garantindo que os usuários tenham apenas os privilégios de acesso permitidos. Quando os usuários entram na rede com um dispositivo e suas credenciais são validadas, não precisam de nova autenticação. Eles permanecem conectados enquanto o dispositivo estiver ligado e o sistema aplicar automaticamente a política para esse usuário.

As políticas garantem que todos os usuários, dentro ou fora da organização, tenham acesso apenas às áreas permitidas e que os controles de acesso sejam aplicados de forma consistente. Elas também descomplicam os fluxos de trabalho da empresa, enquanto reforçam a segurança cibernética. Os usuários podem acessar rapidamente os sistemas e informações de que precisam, sem procedimentos onerosos de login de segurança.

Reduzir a vulnerabilidade do dispositivo

As empresas se conectam a muitos dispositivos IoT. A solução Alcatel-Lucent Enterprise Digital Age Networking permite que as organizações façam a conteinerização de cada dispositivo, criando um segmento de rede virtual para evitar que qualquer dispositivo se torne um ponto de ataque. A conteinerização dentro da Digital Age Networking faz múltiplas redes virtuais a partir de uma única rede física, é simples para a TI implementar e é gerenciada por um único sistema de gerenciamento. A solução descobre automaticamente cada dispositivo na rede. Quando um dispositivo é conectado à rede, o Alcatel-Lucent OmniVista® Network Management System, disponível localmente ou na nuvem, tenta identificar o dispositivo. Se o sistema de gerenciamento não tiver o dispositivo em seu banco de dados, ele consultará um banco de dados na nuvem que contém mais de 29 milhões de dispositivos.

Uma vez identificado o dispositivo, o sistema irá classificá-lo, por exemplo, como uma câmera de segurança. Se esse dispositivo estiver na lista de fornecedores aprovados para câmeras de segurança, ele será adicionado à rede. Se não, então ele não será conectado. A solução é então configurada em um contêiner virtual para o dispositivo, segmentando-o do resto da rede. Se alguém invadir qualquer dispositivo em rede, esse invasor não conseguirá usar esse dispositivo para acessar o restante da rede.

Inteligência artificial para um ambiente de confiança

Uma vez conectados, os dispositivos devem ser monitorados continuamente para identificar quaisquer ameaças e manter a confiança. A análise e a visibilidade da aplicação da ALE permitem aos administradores ver o que se passa na rede, por dispositivo. A análise identifica padrões para o comportamento normal e esperado da rede, bem como quaisquer padrões incomuns quando eles ocorrem. O comportamento dos aplicativos na borda da rede podem ser monitorados para decidir se devemos conectar à aplicação, assim como detectar qualquer comportamento incomum em aplicações autorizadas, como por exemplo uma câmera de vídeo que está produzindo mais dados do que deveria.

Se uma anomalia ou comportamento incomum ocorrer no dispositivo, a análise mostrará esses dados para que o gerente de segurança da rede possa intervir. Hoje, a investigação deve ser feita manualmente, mas a ALE está trabalhando na automatização da resposta usando AI e ML.

Proteja a rede

Embora as organizações hoje estejam cientes da necessidade de proteger os dispositivos IoT na rede, elas podem deixar de considerar os dispositivos que formam a base da rede, como switches e access points. A Alcatel-Lucent Enterprise emprega muitas tecnologias para reduzir a ameaça desses dispositivos. Soluções ALE:

- Fortalecem o software do sistema operacional para fornecer código seguro e diversificado
- Enviam o software do sistema operacional para verificação e validação por terceiros para garantir que não existam pontos de entrada ou backdoors fáceis
- Garantem que, toda vez que um switch seja inicializado, a memória seja compilada e ativada de uma maneira diferente. Embora os switches funcionem de forma idêntica, não há dois deles com a mesma configuração de memória internamente. Se alguém violar um switch ALE, não poderá acessar outro switch da mesma maneira.
- Proporcionam proteção integrada contra negação de serviço (DoS). A CPU pode detectar quantidades incomuns de tráfego na rede e desligar automaticamente a CPU, se necessário.
- Múltiplas certificações de segurança, como JDIC e FIPS
- Realizar atualizações contínuas de software

Conexões seguras para o tráfego de entrada e saída

Para o tráfego de entrada, nossos recursos de VPN fornecem uma conexão criptografada à rede local, enquanto o tráfego de ponta a ponta é protegido usando a criptografia MACsec (também conhecida como IEEE 802.1AE) para proteger a informação enquanto ela atravessa a rede.

Relatórios

Os relatórios da ALE permitem que diferentes pessoas tenham acesso a informações sobre o status, desempenho e saúde da rede, como as aplicações estão sendo executadas e a satisfação do usuário. Por exemplo, a TI pode ver dados sobre o desempenho e as operações da rede.

As unidades de linha de negócios podem garantir que equipamentos, como sensores ou sistemas de telemetria, transmitam dados para servidores e tablets perfeitamente. O departamento de TI pode determinar se a rede está fornecendo serviços que permitem que os funcionários passem mais tempo fazendo seu trabalho e se eles estão obtendo o máximo da rede.

A segurança cibernética nos setores da indústria

Setor de Educação

À medida que as instituições de ensino adotam estratégias de campus inteligente, mais dispositivos móveis e conectados serão adicionados às suas redes, e os dispositivos de Internet das Coisas (IoT) acessarão cada vez mais aplicativos e dados além do perímetro da rede.

Conforme a conectividade e a inovação são implementadas em grandes infraestruturas de campus, elas se tornam imediatamente vulneráveis a ameaças cibernéticas. Alcatel-Lucent Enterprise Digital Age Networking para campi inteligentes mantém os ativos de TI e os dados seguros na era da transformação digital de hoje. Com essa solução, as instituições podem gerenciar de perto o acesso do usuário, reduzir as vulnerabilidades criadas pela IoT, dispositivos móveis e de rede, evitar que a violação inevitável forneça um ponto de ataque, ao mesmo tempo que habilita os serviços e aplicativos que seus alunos e funcionários precisam.

Setor de Transportes

Os avanços nos sistemas de transporte resultantes das inovações tecnológicas exigirão a transformação da base existente sobre a qual são construídos. A integração dos dispositivos e sistemas que permitem que qualquer ecossistema de transporte funcione exige conexões rápidas, confiáveis e seguras. As redes de dados de transporte devem estar cientes da IoT para conectar perfeitamente sensores, câmeras, sinalização e sistemas de controle de tráfego. A segurança da rede também é de vital importância para proteger os dados e a integridade da rede.

A ALE usa código diversificado seguro para melhorar a integridade da rede e fornecer segurança adicional contra ataques cibernéticos à rede. O código diversificado seguro protege as redes de vulnerabilidades intrínsecas, exploits de código, malware e back doors potenciais que podem comprometer operações de missão crítica. A ALE também fornece impressão digital de IoT para identificar cada dispositivo, incluindo veículos, sensores e câmeras para garantir que eles não representem uma ameaça à segurança da rede. A estratégia de segurança em profundidade da ALE recebeu os mais altos níveis de certificação de agências governamentais, incluindo Common Criteria (EAL2 e NDcPP), JITC, FIPS 140-2 e NIST.

Setor de Saúde

A área da saúde tem sido, e continua sendo, uma das indústrias mais visadas pelos hackers. E o problema não para de crescer. Em 2018, o setor de saúde viu 15 milhões de registros de pacientes comprometidos em 503 violações, três vezes a quantidade observada em 2017, segundo o Protenus Breach Barometer.[1]

As violações ocorrem porque os dados de saúde são extremamente valiosos. Os registros individuais dos pacientes contêm tudo: incluindo nome, endereços atuais e anteriores, histórico de trabalho, nomes e idades dos parentes de um indivíduo e informações financeiras, como cartões de crédito e números bancários.[2]

A ALE Digital Age Networking fornece uma abordagem multifacetada à segurança cibernética que mantém a confiança com acesso seguro e baseado em políticas aos dispositivos médicos conectados, dados de pacientes e aplicativos de software em todo o ecossistema de saúde.

Setor Público

A expansão da função digital tanto no governo central quanto na cidade turvou a linha de proteção dos ativos digitais que suportam o transporte, manutenção da infraestrutura e monitoramento do ambiente. As políticas governamentais de segurança cibernética para segurança de dados, vulnerabilidade e gerenciamento de confiança precisam ser revistas.

A solução de segurança cibernética da ALE fornece uma abordagem de ponta a ponta, centrada nos serviços de segurança para proteger todas as camadas do serviço, desde a rede até o software. Em relação ao dispositivo, as organizações do setor público podem usar a conteinerização para criar um segmento de rede virtual para evitar que os dispositivos se tornem um ponto de ataque.

Setor de Hotelaria

O crescimento da IoT no setor de hotelaria traz uma explosão de ameaças à segurança cibernética, à medida que a proliferação de sensores e dispositivos conectados expande muito a superfície de ataque da rede. A IoT é especialmente suscetível porque muitos dispositivos IoT são fabricados sem segurança em mente ou construídos por empresas que não entendem os requisitos de segurança atuais. Consequentemente, os sistemas IoT passam a ser o elo mais fraco em segurança de rede para empresas de hotelaria.

A proteção do tráfego e dos dispositivos IoT requer uma abordagem estratégica que aproveite as vantagens de várias proteções de segurança. Para ajudar hotéis, cassinos, resorts e outras empresas de hospitalidade a aproveitar os benefícios e mitigar os riscos da implantação de IoT, a ALE fornece uma estratégia de segurança de vários níveis que oferece proteção em todas as camadas da infraestrutura, desde o usuário e dispositivo individual até a camada de rede. Também fornece uma estratégia de contenção de IoT para simplificar e proteger a integração de dispositivos e fornecer os recursos de rede certos para executar o sistema de maneira adequada e eficiente, tudo em um ambiente seguro para proteger as empresas de hospitalidade contra ataques cibernéticos.

1 https://healthitsecurity.com/news/the-10-biggesthealthcare-data-breaches-of-2019-so-far
2 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-tohackers/#2bb1f96b50cf

Summary

Digital transformation has profoundly changed enterprise cybersecurity requirements as the number of connected devices increases, the network perimeter disappears, and change continues to accelerate. Alcatel-Lucent Enterprise Digital Age Networking keeps your IT assets and data secure in today's digital transformation age. With this solution, you can closely manage user access, reduce vulnerabilities created by IoT, mobile and network devices, keep the inevitable breach from providing a point of attack and provide a trusted enterprise ecosystem.