ALE | Where Everything Connects

A segurança cibernética no campus na era da IoT e do GDPR

Alcatel·Lucent Enterprise

Índice

Introdução

A segurança cibernética no campus é um tópico "top of mind" permanente no mercado do ensino superior. Pela segunda vez em três anos, a segurança das informações foi o tema principal da pesquisa anual "Top 10 IT Issues" da Educause, realizada com CIOs do setor de ensino superior[1]. Isso não deveria ser uma surpresa, de acordo com o mais recente relatório da Verizon referente a investigações de violações de dados (DBIR - Data Breach Investigations Report)[2]. O relatório, que demonstra uma tendência de crescimento em atividades cibernéticas criminosas, identifica os três setores mais afetados por tais atividades: Finanças e seguros, Saúde e Educação.

A segurança das informações na educação sempre teve que lidar com a disputa entre facilidade de uso e segurança total; às vezes, a segurança ganha, mas normalmente a prioridade fica para a facilidade de uso. Levando em consideração a nova legislação de privacidade da Europa, conhecida como Regulamento Geral sobre a Proteção de Dados (GDPR - General Data Protection Regulation)[3, 4] e a introdução de uma ampla variedade de dispositivos de IoT, não é nem um pouco surpreendente que a segurança das informações e a proteção da reputação das instituições sejam fatores extremamente importantes para os CIOs das instituições de ensino superior.

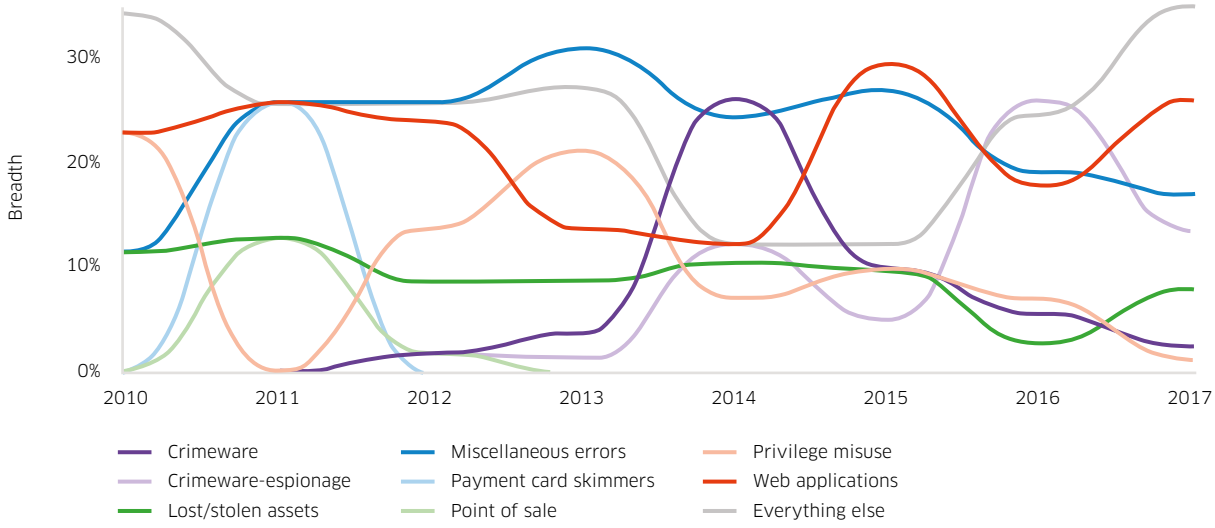
Esse enfoque na segurança das informações é providencial. Nunca antes a tecnologia da informação teve um papel tão importante na educação. Seja ao pesquisar sobre um tópico para uma aula ou para entregar uma tarefa, a tecnologia da informação está no âmago da pedagogia, bem como as estratégias implementadas para identificar e ajudar com o sucesso acadêmico dos alunos.

O relatório de 2018 da Verizon referente a investigações de violações de dados fornece insights muito interessantes sobre os vetores de ataque e as motivações para atividades cibernéticas mal-intencionadas.

Tabela 1. Resumo de violações de dados do setor de educação em 2017

Frequência	292 incidentes, sendo 101 com divulgação de dados confirmada
Os três padrões principais	Fatores genéricos, Ataques a aplicativos Web e Erros diversos representam 76% das violações
Agentes de ameaça	Externos (81%), Internos (19%), Parceiros (2%), Várias partes (2%) (violações)
Motivos dos agentes	Financeiros (70%), Espionagem (20%), Diversão (11%)
Dados comprometidos	Pessoais (72%), Segredos (14%) e Médicos (11%)

Figura 1. Padrões observados em violações no setor de educação



1 EDUCAUSE Center for Analysis and Research (ECAR), "Top 10 IT Issues 2018," EDUCAUSE Research Snapshot, *EDUCAUSE Review*, 29 de janeiro de 2018.
2 Verizon Enterprise, "Verizon Data Breach Investigations Report (DBIR) 2018", abril de 2018, páginas 29-30
3 https://eugdpr.org
4 https://gdpr-info.eu

Este white paper explora a implementação de estratégias de segurança com base em riscos, como o conceito de "defesa avançada". Esse conceito promove a proteção de uma rede de computadores com uma série de mecanismos de defesa individuais, de modo que, se um ataque for lançado, o invasor precisará transpor várias camadas independentes para ter êxito.

A "tríade CIA" será mencionada ao longo deste relatório. Esse conceito identifica alvos cibernéticos que contêm informações "Confidenciais", afetam a "Integridade" das informações ou negam a "Disponibilidade" (Availability) das informações. A tríade CIA é útil para a formulação de políticas de segurança para todo o campus e para a atribuição de valores de risco. Por exemplo, um laptop roubado ou perdido que contenha informações de identificação pessoal (PII) seria classificado como um ataque de informações confidenciais; um hacker que conseguisse alterar notas com sucesso estaria violando a integridade do sistema de informações dos alunos; além disso, as impressoras BYOD em repúblicas de alunos poderiam ser cooptadas para participar de um ataque de negação de serviço (DoS), o que seria classificado como um ataque de disponibilidade, porque o objetivo de um ataque de DoS é inundar um servidor web com tantos pedidos falsos que o servidor deixa de responder às solicitações legítimas.

Para os fins deste documento, ameaças de segurança das informações serão mencionadas como atividades cibernéticas mal-intencionadas, definidas pelo Governo Federal dos Estados Unidos da América como:

> «Atividades, diferentes daquelas autorizadas pela ou de acordo com a legislação dos EUA, que buscam comprometer ou prejudicar a confidencialidade, integridade ou disponibilidade de sistemas de computadores, informações ou comunicações, redes, infraestrutura física ou virtual controlada por computadores ou sistemas de informações, ou ainda informações residentes nesses sistemas.»

Os efeitos das atividades cibernéticas mal-intencionadas incluem:

> «A manipulação, interrupção, negação, degradação ou destruição de computadores, sistemas de informações ou comunicações, redes, infraestrutura física ou virtual controlada por computadores ou sistemas de informações, ou ainda informações residentes nesses sistemas.»

O ano de 2018 representou um marco com a profusão de dispositivos da Internet das Coisas (IoT) no campus e com a introdução de regulamentos de privacidade no espaço cibernético, mais especificamente o GDPR da União Europeia. O GDPR tem implicações para universidades no mundo todo, e ambos os tópicos serão discutidos em profundidade.

Regulamento Geral sobre a Proteção de Dados

O GDPR foi aprovado em 25 de maio de 2018, pela União Europeia, para devolver aos cidadãos o controle de suas informações cibernéticas. Essencialmente, o GDPR concede a cada residente da UE o direito de conhecer e decidir como seus dados pessoais estão sendo utilizados, armazenados, protegidos, transferidos e excluídos. Os indivíduos também têm o "direito de serem esquecidos", solicitando a exclusão de todos os seus dados. Ao contrário da definição de informações de identificação pessoal usada por outros países, o GDPR também engloba os dados de localização, incluindo endereços IP – o que pode ter um grande impacto sobre a implantação de Serviços Baseados em Localização (LBS - Location Based Services) no campus ou até mesmo em logs de equipamentos de rede.

Sendo a legislação de privacidade mais avançada do mundo, além dos direitos especificados acima, o GDPR também tem o expediente de impor qualquer não conformidade. As violações ao GDPR podem resultar em penalidades por não conformidade de 4% da receita mundial anual ou US$ 23 milhões, o valor que for maior.

O planejamento para o GDPR seria incluído na seção de Confidencialidade da tríade CIA e será abordado mais especificamente na seção Segurança dos aplicativos.

Internet das Coisas (IoT)

A Internet das Coisas é um tópico interessante. Ao contrário dos sistemas de rede definidos por software (SDN - Software-Defined Networking), que contavam com a consistência de implementação na comunidade de rede, os dispositivos da IoT já fazem parte do campus, e o espaço ocupado por eles continuará a crescer. Um dispositivo de IoT é um dispositivo conectado que tem a capacidade de enviar e/ou receber informações sem a necessidade de intervenção humana para operá-lo. Em um campus, isso pode incluir uma impressora Wi-Fi de consumo, câmeras de segurança e sensores de IoT ou até mesmo projetores para auditórios/salas de aula.

Sob uso normal, esses dispositivos são essencialmente inócuos. No entanto, por serem dispositivos de rede e terem um sistema operacional, eles são sensíveis a ataques de hackers e malware – o que os coloca em risco de serem incluídos e usados em um exército de bots. Talvez você se lembre do ataque de DDoS (negação de serviço distribuído) de outubro de 2016[5] contra a Dyn, um provedor de serviços de nomes de domínio com base nos EUA e com clientes na Europa e na América do Norte. A Dyn foi atacada três vezes no mesmo dia. A análise resultante confirmou que dispositivos de IoT (câmeras, babás eletrônicas, roteadores Wi-Fi e impressoras) foram comprometidos com uma variante de malware baseada no código-fonte do vírus Mirai.

O planejamento para a IoT está relacionado principalmente à seção de Disponibilidade da tríade CIA e será abordado mais especificamente na seção Segurança de acesso à rede.

Defesa avançada

A defesa avançada é a prática de proteger um computador com camadas de dispositivos ou estratégias independentes de segurança. Ela foi originalmente concebida pela National Security Agency (NSA) dos EUA como uma abordagem abrangente para a proteção das informações. Existem três áreas de enfoque nesse conceito:

1. Pessoas: a garantia das informações é o objetivo da liderança de TI e inclui a aplicação de serviços de segurança, como disponibilidade, integridade, autenticação, confidencialidade. A aplicação desses serviços deve ser baseada no paradigma de Proteger, Detectar e Reagir. Também incluídas aqui estão a aplicação/ativação de práticas e treinamentos.
2. Tecnologia: inclui hardware e software que impedem o acesso ao conteúdo de um sistema.
3. Operações: concentra-se em todas as atividades necessárias para sustentar a postura de segurança de uma organização no dia a dia e pode incluir avaliações de segurança, recuperação e reconstituição do sistema, controle de mudanças e manipulação de dados.

O restante deste white paper explorará essas áreas de enfoque por meio da análise das seguintes camadas: Segurança de borda da rede, Segurança dos aplicativos, Segurança da rede LAN, Segmentação de rede e Gerenciamento de rede.

Segurança na borda da rede

A borda da rede é onde a rede interna da instituição faz interface com outra rede, incluindo uma operadora, REN ou Internet pública. Esta é a primeira camada de uma arquitetura de defesa profunda. Essa camada também pode ser vista como aquela que garante a proteção das informações contra os "Bárbaros no portão" e suas atividades mal-intencionadas.

A borda da rede tem tráfego de entrada e saída, o que significa que teremos que lidar com cada tipo de tráfego.

5 https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

Tráfego de entrada

Tráfego de entrada: seja o tráfego de um link de WAN, da Internet pública ou de um link de rede de pesquisa, algumas ou todas as seguintes tecnologias são aplicáveis:

1. Firewall: residindo normalmente na DMZ (zona desmilitarizada), um firewall pode realizar várias tarefas de segurança, incluindo NAT (conversão de endereços de rede), VPN (rede virtual privada) e, certamente, aplicar a lógica de segurança para o tráfego.
2. Sistema de detecção de invasões (IDS)/Sistema de detecção e prevenção de invasões (IDPS): são importantes para proteger a rede contra ataques. Existem dois tipos:
    1) Um com base em assinatura, que reconhece padrões de explorações conhecidas
    2) Outro com base em anomalias, que reconhece os desvios da atividade de rede básica
3. Rede virtual privada (VPN): fornece uma conexão criptografada com a rede local. Esse tipo de conexão é o melhor para comunicações seguras e geralmente emprega esquemas de autenticação multifator (MFA).
4. Filtros de SPAM: considerados por muitos como o firewall de um servidor de emails. Os filtros de SPAM ganharam mais sofisticação e recursos capazes de identificar anexos infectados por malware, endereços falsos (phishing) e outros tipos de ataques. De acordo com o relatório da Verizon sobre violações de dados, o phishing é um dos principais vetores de ataque no setor de ensino superior. Implementar um filtro de SPAM pode ajudar a reduzir o número de ataques.
5. Filtro de tráfego da Web: alguns firewalls podem realizar essa tarefa. Por isso, nem todas as instituições implementam um filtro de tráfego da Web. No entanto, essa tecnologia pode permitir que uma universidade conceda ou negue o acesso a sites em sua rede. Mais comumente observado no ramo de ensino fundamental e médio, este dispositivo de segurança ajuda a manter os usuários longe de sites que podem causar infecção ou perda de controle.
6. Monitoramento de segurança da rede: aplicativos como o Bro[6] ou o Splunk[7] podem fornecer dados úteis sobre o tráfego de rede e sobre anomalias potenciais de segurança.

Tráfego de saída

Além de solicitar o tráfego, uma rede também envia informações para fora dela. Embora esse tipo de tráfego não seja normalmente suspeito, monitorá-lo poderá ajudar a informar a instituição caso ocorra uma violação de segurança (como no caso de dispositivos da IoT comprometidos com malware e participando de ataques de DDoS).

O tráfego de saída deve atravessar as defesas do tráfego de entrada, mas existe uma tecnologia que é útil para proteger o tráfego de saída: a criptografia.

1. A criptografia MACSec é também conhecida pela designação 802.1AE do IEEE. Essa tecnologia oferece suporte a transmissões criptografadas através de um link. Por exemplo, se você tiver um site de recuperação de desastres (DR) para seu data center, poderá preencher esse site usando um link MACSec criptografado, garantindo a confidencialidade, a integridade e a autenticação da origem dos dados.

Segurança dos aplicativos

A próxima camada que ajuda você a lidar com as atuais ameaças de segurança cibernética é a segurança dos aplicativos. Essa camada engloba tanto dispositivos de computação do usuário final quanto aplicativos baseados em rede. A segurança dos aplicativos é uma importante ferramenta no arsenal de segurança de uma universidade. Ela lida com os domínios de confidencialidade e integridade da tríade CIA e é um fator importante para a implementação das proteções do GDPR.

6 https://www.bro.org

7 https://www.splunk.com

Entre as tecnologias e táticas dessa camada estão:

1. Criptografia de dados: os dois principais sistemas operacionais para PCs têm recursos de criptografia de dados em disco. Esse é um recurso importante, uma vez que protege os dados dos usuários contra acesso casual. A criptografia do armazenamento em rede está ficando cada vez mais popular e melhora a integridade e a confidencialidade das informações.
2. Autenticação multifator (MFA): a autenticação multifator é um mecanismo que requer que dois dispositivos trabalhem em conjunto para acessar um aplicativo ou recurso com êxito. Normalmente, o fluxo consiste em uma ID de usuário e senha e, em seguida, uma série de números é fornecida e enviada como texto para o smartphone do usuário. Isso possibilita mais uma camada de confirmação de que o usuário é realmente quem diz ser. Outro mecanismo para oferecer MFA é usar tokens de hardware, como os da RSA e da Google, em vez de texto pelo smartphone. Essa estratégia tem a vantagem de poder ser utilizada na VPN e com outras estratégias de comunicação segura.
3. Microssegmentação: o data center evoluiu de servidores físicos para servidores virtuais, com dúzias de servidores virtuais ocupando o espaço de um ou dois servidores físicos. No entanto, os riscos aumentam com essa densidade. Os firewalls tradicionais com inspeção de estado não têm a capacidade de analisar, em alta velocidade, os fluxos de tráfego de um data center. A VMWare[8], um importante provedor de hipervisores, implementou uma tecnologia chamada "microssegmentação". Isso significa que, agora, cada aplicativo pode ter seu próprio perímetro de segurança sem depender exclusivamente das VLANs.

As práticas implementadas nessa camada devem incluir:

4. Treinamento de conscientização sobre segurança para o usuário final: essa atividade é geralmente realizada durante o mês de conscientização sobre segurança (outubro). No entanto, lembretes periódicos sobre explorações de phishing, spear phishing e engenharia social (que resultam na divulgação de credenciais) devem ser fornecidos ao longo de todo o ano para ajudar a reduzir a área de superfície desse vetor de ataque.
5. Patches de segurança: é importante testar os patches de segurança e as atualizações de aplicativos antes de aplicá-los. No entanto, as releases do fabricante são importantes e devem ser priorizadas. De acordo com o relatório da Verizon sobre violações de dados, 6% dos ataques bem-sucedidos exploram brechas de segurança que um patch poderia evitar. Na verdade, alguns dos ataques mais prejudiciais ocorreram devido ao adiamento das aplicações de patches.

Segurança de acesso à rede

As redes locais (LAN) e as redes locais sem fio (WLAN) são pontos de entrada para os usuários de computadores do campus. Normalmente, uma conexão de LAN conecta fisicamente um cabo Ethernet do dispositivo de rede até um conector RJ-45 de parede. Uma conexão de WLAN não requer conectividade física. Em vez disso, ela usa o chip Wi-Fi interno do dispositivo para detectar e se conectar à rede.

As universidades sempre tiveram que buscar um equilíbrio entre facilidade de uso e segurança total. É importante não tornar o acesso seguro algo muito complicado, caso contrário os estudantes e outros usuários poderão tentar encontrar uma solução alternativa ou aumentar a quantidade de dispositivos de "TI de sombra". Por exemplo, em alguns campi, um convidado precisará de um patrocinador para conseguir se autenticar na rede; em outros, é comum enviar o convidado para um portal de autoatendimento onde ele poderá inserir informações pessoais, concordar com a linguagem de uso aceitável e, em seguida, entrar. Ambos os métodos fornecem a mesma proteção para a rede, mas um deles é um pouco mais oneroso do que o outro.

8 https://www.vmware.com

Em uma arquitetura de defesa avançada, a segurança de acesso à rede é um dos investimentos mais importantes a se fazer. Essa camada tem tudo a ver com os 4 As: Autenticar, Autorizar, Auditar e Administrar. A autenticação bem-sucedida leva à autorização para acessar os recursos de rede permitidos para uma função específica. A auditoria está relacionada ao monitoramento do comportamento e do tráfego de rede. Se esse comportamento não for normal, será necessário administrar regras de quarentena ou de tráfego de rede.

As tecnologias de segurança de acesso à rede que oferecem suporte aos 4 As incluem:

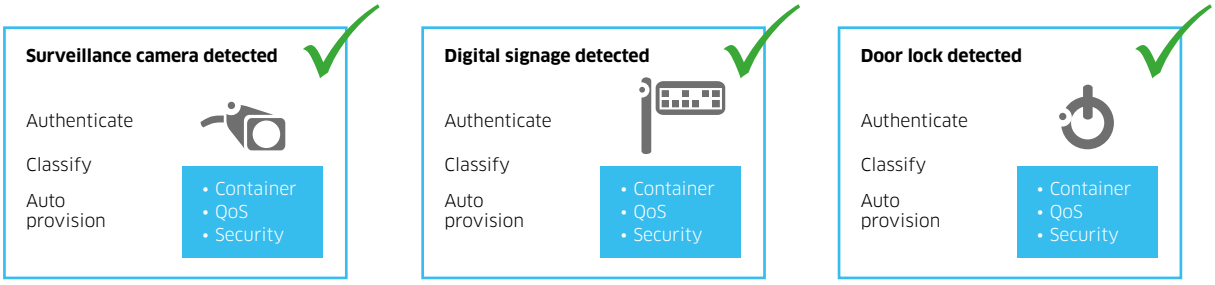
1. 802.1X: um mecanismo de controle de acesso à rede padrão do IEEE e com base em porta que fornece um mecanismo de autenticação para dispositivos conectados à LAN e à WLAN. O 802.1X requer um suplicante (computador ou dispositivo que solicita o acesso); um autenticador (geralmente o switch Ethernet ou o AP ou controlador de WLAN); e um servidor de autenticação (geralmente um servidor RADIUS ou EAP). O suplicante fornece as credenciais ao servidor de autenticação. Se elas estiverem corretas, o autenticador concede o acesso à rede.
2. Biometria: um novo método de autenticação de segurança potencialmente mais fácil de usar é a utilização de dados biométricos ou de algo que seja exclusivo do usuário, como impressões digitais, reconhecimento de íris ou detecção de timbre de voz. Embora esse método não sirva para os dispositivos da IoT, ele fornece uma maneira fácil de conceder acesso à rede a uma pessoa.
3. Criptografia: embora tenha sido anteriormente mencionada como um mecanismo de segurança para dados em repouso e em trânsito entre data centers, a criptografia MACSec está se tornando mais predominante na LAN – do núcleo até a borda. Além disso, os padrões de WLAN do IEEE adotaram a criptografia com o padrão 802.11i, que protege as transmissões Wi-Fi do access point até o usuário contra ataques do tipo Man-in-the-Middle (uma das principais razões para não se utilizar conexões Wi-Fi públicas e sem criptografia). E, recentemente, a Wi-Fi Alliance anunciou o WPA3 (Wi-Fi Protected Access 3). O WPA3 adiciona novos recursos para simplificar a segurança do Wi-Fi, habilitar uma autenticação mais robusta, oferecer mais potência à criptografia para os mercados de dados altamente confidenciais e, ao mesmo tempo, manter a resiliência das redes de missão crítica.
4. Sistemas operacionais mais robustos: muitos dispositivos de rede são adquiridos com perfis de autenticação de administrador padrão. Infelizmente, e mais frequentemente no caso dos dispositivos da IoT, esses padrões nunca são alterados, tornando o dispositivo um alvo fácil para inserção de malware ou até mesmo para mudar códigos. Um sistema operacional mais robusto para dispositivos é aquele que mistura o código e a localização da memória para que uma falha bem-sucedida de um dispositivo não seja repetida com êxito de maneira automática. Além de proteger a integridade do dispositivo, um sistema operacional mais robusto também pode apresentar os seguintes recursos:
    1) Reconhecimento e mitigação de ataques de DoS: alguns dispositivos de infraestrutura de rede são capazes de reconhecer que um ataque de DoS está em andamento e imediatamente impedir o ataque, interrompendo o tráfego ilegal.
    2) Reconhecimento de ataques com base em IP: alguns dispositivos de infraestrutura de rede são capazes de se integrar com o SNORT ou com outros produtos de IDS/IDP e reagir a uma assinatura positiva de ataque de IP e colocar o tráfego inválido em quarentena.
5. Políticas unificadas de acesso à rede: após a autenticação com êxito, essa estrutura autoriza o acesso à rede com base em alguns parâmetros, como endereço MAC, hora do dia, função do usuário, departamento (por exemplo, de alunos, convidados, professores, funcionários, fornecedores, administração, admissões, atlética) ou até mesmo a localização na qual ocorreu a autenticação. Essa estrutura é compatível com o acesso à LAN e à WLAN. Ela acaba com a falta de correspondência e com a duplicação de perfis de segurança e fornece acesso consistente e seguro à rede.
6. Dispositivos da IoT: as políticas unificadas de acesso à rede são um recurso essencial para a capacitação de dispositivos da IoT. Além disso, o recurso de impressões digitais do dispositivo DHCP pode identificar rapidamente dispositivos da IoT de vários fabricantes. Esse recurso aproveita as opções do DHCP que fornecem informações específicas do fornecedor sobre o hardware ou o sistema operacional do dispositivo. A troca é feita usando as opções do DHCP conforme definido pela RFC 2132.[9] Ao utilizar as opções do DHCP, você tem informações sobre

9 http://www.ietf.org/rfc/ rfc2132.txt

fornecedor, dispositivo e sistema operacional, que juntas constituem a “impressão digital” do dispositivo. Por exemplo, uma recente RFP de CCTV foi concedida a um único fabricante. Esses novos produtos coexistirão com as câmeras CCTV existentes. Com a implementação do UNAP, a equipe de segurança tem duas maneiras de identificar e aplicar regras de segurança de rede: via impressão digital DHCP ou mascaramento de endereço MAC. O mascaramento de endereço MAC usa os primeiros 24 bits do endereço MAC, que contém o OUI (Organizationally Unique Identifier)[10]. Ao usar o UNAP com uma política de mascaramento de endereço MAC, a instituição poderá configurar com rapidez e segurança suas novas câmeras de vigilância. As impressões digitais DHCP permitiriam ao campus identificar todas as câmeras CCTV e aplicar políticas de segurança consistentes.

Geralmente, as impressões digitais do dispositivo DHCP têm suporte em sistemas de WLAN. No entanto, é mais eficaz ter dispositivos de LAN incluídos, já que nem todos os dispositivos da IoT se conectam à rede via Wi-Fi.

Figura 2. Classificação e reconhecimento automáticos

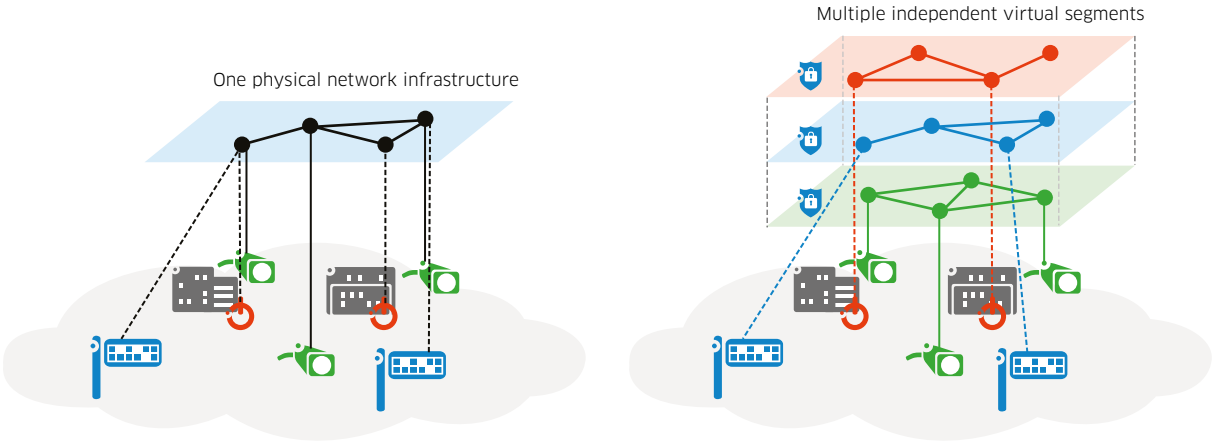


Segmentação de rede

Com a introdução dos switches de LAN, a segmentação de rede foi expandida da segmentação física para incluir LANs virtuais (VLANs). Isso permite limitar os serviços de rede aos usuários que sejam membros da VLAN, protegendo, essencialmente, aplicativos e serviços. A maioria dos equipamentos de rede oferece suporte a até 4.096 VLANs, o que deve ser mais do que suficiente. Mas, na realidade, isso pode ser algo desafiador e, por isso, a rede deve ser projetada adequadamente.

O problema da exaustão da VLAN é real e tem sido abordado em várias tecnologias usadas pelos campi. O MPLS (Multiprotocol Label Switching)[11] e seu derivado, o Shortest Path Bridging (SPB – IEEE 802.1aq)[12] usam o conceito de “interfaces de serviço” para segmentar ainda mais as atividades de rede.

Figura 3. SPBM – Segmentação de rede, sem Spanning Tree



10 http://standards-oui.ieee.org/oui/oui.txt
11 https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
12 https://en.wikipedia.org/wiki/IEEE_802.1aq

Gerenciamento de rede

O gerenciamento de rede é um aplicativo frequentemente negligenciado pelos fornecedores de equipamentos de infraestrutura. Há muitas razões para isso. A principal delas é a predominância de aplicativos de terceiros para gerenciar ambientes de vários fornecedores. No entanto, é preciso analisar o outro lado da moeda ao se utilizar um sistema de gerenciamento de rede (NMS) de terceiros. Muitas plataformas de NMS de terceiros podem se integrar aos direitos de suporte e até mesmo sugerir versões de manutenção capazes de solucionar erros potenciais na implantação. Além disso, o NMS de OEM pode fornecer uma grande variedade de estatísticas, análises e tendências que podem possibilitar um gerenciamento de rede proativo.

Os profissionais de TI que atuam na área de educação também estão começando a buscar recursos de Deep Packet Inspection (DPI) para a infraestrutura de LAN. A capacidade de saber quais aplicativos estão consumindo mais largura de banda pode informar ao departamento de TI quais são as áreas que precisam de investimentos. Por exemplo, se o tráfego de/para o aplicativo LMS for o principal consumidor da largura de banda, provavelmente seria uma boa ideia verificar os recursos atribuídos à VM do LMS. Ou, se o aplicativo for baseado na nuvem, é recomendável investigar a experiência do usuário e determinar se mais investimentos são necessários para aumentar a largura de banda, a memória, a capacidade de processamento ou o armazenamento.

Em relação à segurança cibernética no campus, o NMS é a plataforma onde tudo começa. De permitir o acesso à CLI SSL/criptografada até todo o equipamento de infraestrutura, a implementação de políticas unificadas de acesso à rede, o monitoramento de tráfego em busca de anomalias e a quarentena de dispositivos/usuários que apresentam mau comportamento, o NMS é a plataforma que pode fazer tudo isso e muito mais.

Além de ter um NMS robusto, alguns programas de terceiros devem ser considerados:

1. perfSONAR[13]: embora essa ferramenta seja usada por muitas instituições de pesquisa, ela apresenta recursos que podem ajudá-lo a entender o desempenho da sua rede completa. Aqui está um trecho sobre o que essa ferramenta pode fazer:

   "Garantir que as coisas funcionem bem, de ponta a ponta, é essencial. O monitoramento dentro de um único domínio é uma prática comum e bem aceita; o monitoramento de desempenho entre domínios é algo difícil de realizar usando as ferramentas tradicionais. O perfSONAR é uma infraestrutura de teste e medição que pode ser amplamente implantada e usada por redes e instalações científicas ao redor do mundo para monitorar e garantir o desempenho da rede."
2. Ferramentas dentro do perfSONAR que oferecem solução de problemas adicional:
   1) pScheduler: testes de taxa de transferência para locais remotos
   2) OWAMP: verificações contínuas de latência e perda de pacotes

Resumo

As instituições de ensino são o terceiro setor do mundo mais afetado por problemas de segurança. A segurança cibernética no ensino não é algo opcional. Ela é uma dimensão essencial na arquitetura corporativa e pode contribuir para o reconhecimento positivo da marca de uma universidade.

Implementar um plano de segurança com base em riscos permite que a universidade aloque seu orçamento de acordo com a necessidade ou os riscos. Além disso, a arquitetura de defesa profunda garante que um invasor tenha que superar diferentes tecnologias durante a exploração para ter êxito.

Empregar as classificações da tríade CIA de Confidencialidade, Integridade e Disponibilidade (Availability) em seus ativos cibernéticos ajuda a determinar o risco da instituição e um peso para o tópico.

A implementação dos 4 As (Autenticação, Autorização, Auditoria e Administração) oferece uma estrutura unificada para o acesso à rede e o comportamento tanto em redes LAN quanto em redes WLAN.

A segmentação da rede com MPLS ou SPB permite o controle granular de serviços e dos usuários/dispositivos que acessam esses serviços.

13 https://www.perfsonar.net/about/what-is-perfsonar/

Por fim, o treinamento, a arquitetura e a tecnologia de segurança conduzirão você por um longo caminho para proteger seus ativos. No entanto, conforme identificado em muitos estudos, phishing e erros do usuário são os métodos de violação mais proeminentes. Treinar alunos, professores, funcionários e fornecedores sobre segurança cibernética pode ajudar a reduzir seu fator de risco número um.

Referências e recursos

National Institute of Standards and Technology: este link leva você para a página inicial da estrutura de segurança cibernética do NIST: https://www.nist.gov/cyberframework

EDUCAUSE: uma associação sem fins lucrativos que ajuda o setor de ensino superior a aumentar o impacto da TI. Os resultados da pesquisa anual "Top 10 IT Issues" de 2018 e links para outros recursos podem ser encontrados aqui: https://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education

Alcatel·Lucent Enterprise