NOTA SOBRE A APLICAÇÃO

Proteção da infraestrutura crítica

Criptografia de rede para concessionárias

A segurança cibernética apresenta problemas que se tornarão cada vez mais frequentes, complexos e desafiadores. De acordo com Michael Mullen, ex-chefe do Estado-Maior Conjunto das Forças Armadas dos Estados Unidos, "A ameaça cibernética é a única maior ameaça existencial que anda por aí" porque "de fato, a cibernética, para além da simples teoria, pode atacar nossa infraestrutura, nossos sistemas financeiros".[1]

As concessionárias de energia enfrentam elevados desafios cibernéticos, uma vez que são consideradas infraestrutura nacional crítica, que é definida como "tão vital para os Estados Unidos que a incapacidade ou destruição de tais sistemas e ativos teria um impacto debilitante sobre a segurança, segurança econômica nacional, saúde pública nacional, ou proteção".[2]

Para ilustrar os desafios cibernéticos em curso enfrentados pelas concessionárias, uma pesquisa da Unisys de 2014 com o Ponemon Institute mostrou que quase 70% dos fornecedores de infraestrutura crítica pesquisados (concessionárias responsáveis pelo fornecimento de energia, água e outras funções críticas do mundo) relataram pelo menos uma violação de segurança que levou à perda de informações confidenciais ou interrupção das operações nos últimos 12 meses.[3]

A segurança é essencial para estabelecer e manter a confiança do público nas redes elétricas nacionais. A criptografia, uma das principais ferramentas do kit de ferramentas de segurança cibernética, torna as informações ilegíveis para qualquer pessoa, exceto para aqueles que possuem a chave correta para decifrar a mensagem.

A maioria das organizações protege os dados em repouso, protegendo servidores, bancos de dados, roteadores e switches. Para isso, gerenciam o acesso do usuário e o credenciamento. No entanto, nas redes da concessionária de hoje, grandes quantidades de dados críticos são transmitidos como comunicações de alta largura de banda além das paredes da subestação da concessionária ou do data center, atravessando redes regionais e nacionais. Por tanto, uma abordagem de segurança de TI abrangente deve incluir uma solução robusta de criptografia de dados em trânsito (in-flight) como parte de sua estratégia holística de segurança. Com a criptografia dos dados quando eles deixam a segurança da nuvem privada, as operadoras podem assegurar que esses dados ficarão protegidos da interceptação não autorizada ao atravessar a rede, cruzando variados níveis de segurança até atingirem seu destino.

1 CNN: "Admiral Michael Mullen: Farewell and thank you" by Micah Zenko, Nov. 11, 2011; http://globalpublicsquare.blogs.cnn.com/2011/09/29/admiral-michael-mullen-farewell-and-thank-you/
2 Cornell University Law School, Legal Information Institute: U.S. Code 5195c – Critical infrastructures protection; http://globalpublicsquare.blogs.cnn.com/2011/09/29/admiral-michael-mullen-farewell-and-thank-you/
3 Instituto Ponemon: "Unisys Survey Reveals Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year", Julho 10, 2014; http://www.unisys.com/offerings/security-solutions/News%20Release/Unisys-Survey-Reveals-Critical-Infrastructure-Providers-Breached

Benefícios

- Protege os dados em trânsito (in-flight) da concessionária contra a violação de dados e mantém os sistemas críticos seguros
- Protege reputações valiosas e evita multas caras, exposição na mídia pública e rotatividade de clientes, atendendo às expectativas de proteção de informações
- Atende aos requisitos de segurança NERC-CIP para o setor de serviços públicos

Por que os CIOs das concessionárias de serviços públicos não criptografam dados em trânsito

Muitos CIOs das concessionárias de serviços públicos não são totalmente conscientes que, uma vez que os dados deixam a subestação ou data center, eles estão basicamente fora de seu controle. Devido a todos os esforços para bloquear os dados em repouso com firewalls, software antivírus e detecção de intrusão, os criminosos cibernéticos estão cada vez mais voltando sua atenção para a interceptação dos dados conforme eles trafegam pela rede. As empresas de segurança cibernética estão relatando um número crescente de incidentes cibernéticos com foco em redes corporativas e internas.

Outro motivo para a falta de foco na criptografia em trânsito é que muitos CIOs foram levados a acreditar que suas redes de fibra óptica são inerentemente imunes a violações. Na realidade, um hacker com conhecimento intermediário, dispondo de equipamento e software de baixo custo, é capaz de interceptar os dados da concessionária, podendo levar dias, meses ou até anos até que seja notado. Qualquer pessoa com acesso à Internet pode facilmente comprar online uma ferramenta para grampear a fibra e, depois de assistir a alguns tutoriais no YouTube que o orientam sobre o processo de grampeamento, pode aprender rapidamente como roubar dados confidenciais de um cabo de fibra óptica. Vários vídeos que mostram a facilidade com que hackers podem violar uma rede de fibra podem ser encontrados no YouTube. Um único fio de fibra pode transportar uma enorme quantidade de dados e, como os cabos de fibra óptica são surpreendentemente acessíveis, eles se tornaram alvos valiosos para os invasores.

Como invadir uma linha de fibra ótica em minutos **Assista ao vídeo**

Mais um motivo pelo qual os CIOs das concessionárias relutam em implantar a criptografia de dados em trânsito é a preocupação com a redução do desempenho e do custo da rede. Em um setor em que as margens estão diminuindo e a latência da rede pode significar a diferença entre conter ou propagar uma falha no fornecimento de energia, sua preocupação é compreensível, embora infundada. Essas preocupações podem ser decorrentes da experiência com soluções de criptografia de rede de Camada 2 e superiores. Por exemplo, os dispositivos de criptografia da Camada 3 são projetados para criptografia IPSec (criptografia padrão da Internet). O IPSec usa um processo que coloca em "túneis" o pacote de IP original para criptografar um "cabeçalho". No entanto, os túneis podem resultar em aumento na sobrecarga, complexidade, velocidade e processamento de desempenho da rede.

A solução ideal de criptografia em trânsito (in-flight) para a rede

Independentemente de a criptografia de rede fazer parte de uma rede óptica privada ou de ser fornecida por um provedor de serviços como parte de um serviço gerenciado, entre os pontos principais a considerar incluem-se:

Conformidade regulatória. As concessionárias estão muito cientes das regulamentações que podem ser aplicadas às aplicações realizadas por suas redes. O setor de serviços públicos estabeleceu uma série de especificações de segurança de acordo com os padrões da North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP). Isso inclui tudo, desde a proteção de ativos físicos até a proteção de sua cadeia de suprimentos e ativos de TI. A solução escolhida deve atender aos requisitos de conformidade NERC-CIP para o setor de serviços públicos.

Latência. As especificações para latência no mercado de serviços públicos são mais rigorosas do que outras verticais, pois uma oscilação de energia deve ocorrer com um atraso de menos de 10 ms para evitar a propagação de uma falha no fornecimento de energia. As soluções de criptografia de última geração atendem aos requisitos das concessionárias, fornecendo latências baseadas em hardware da ordem de vários microssegundos.

Gestão. Independentemente de os links criptografados serem gerenciados pela concessionária ou provedor de serviços, o "proprietário" dos dados (a concessionária) deve manter o controle das chaves de criptografia, emitir novas chaves conforme necessário e ter visibilidade dos alarmes de segurança e logs associados a seus links criptografados. Isso é possível com a separação do gerenciamento de rede do gerenciamento de chave de criptografia. Se o serviço criptografado for adquirido de um provedor de serviços, o provedor gerenciará os links e seu provisionamento, administração e monitoramento de desempenho, mas não terá controle da distribuição ou manutenção das chaves. Dependendo das políticas de segurança da concessionária, a distribuição de chaves pode ser realizada manual ou automaticamente em túneis criptografados seguros.

Uma abordagem de segurança completa deve abranger não apenas "dados em repouso", incluindo dados que residem em bancos de dados, arquivos e sistemas de armazenamento, mas também criptografia em trânsito, para garantir que os dados sejam protegidos contra detecções não autorizadas ao atravessarem a rede. As técnicas atuais de criptografia em trânsito podem camuflar o tráfego de modo que não possa ser lido ou manipulado e até mesmo disfarçar o fato de que existe um fluxo de tráfego.

Criptografia in-flight na camada óptica

A criptografia de camada óptica resolve todos esses problemas e muito mais. Embora seja verdade que tecnologias como Transport Layer Security (TLS) e Secure Sockets Layer (SSL) são cada vez mais usadas para proteger conexões aos servidores, a única maneira de proteger tudo no link de comunicação dentro e fora de uma instalação é com o uso da criptografia na camada física. Isso é particularmente verdadeiro quando se considera a quantidade de "metadados" gerados por vários serviços em uma rede que não são necessariamente criptografados, mesmo quando se usa criptografia de camada de aplicação, como TLS/SSL. Os endereços IP e MAC, os tipos de protocolo em uso e outras informações de rede são trocados

em sigilo, mesmo quando os dados reais do usuário são criptografados. Esses metadados podem ser usados por adversários para mapear uma rede e planejar ataques, mesmo sem acesso aos dados criptografados da camada de aplicação. Uma abordagem de criptografia em massa da Camada 1 torna todos os dados e metadados da concessionária indecifráveis para qualquer hacker que use a fibra.

Principais aplicações e casos de uso de criptografia para concessionarias:

(1) Comunicações da rede elétrica

a, Teleproteção
b. SCADA

(2) Interconexão de data center

a. Prevenção/recuperação de desastres
b. Consolidação/otimização do data center
c. Mobilidade da carga de trabalho

(3) Transporte de vídeo

a. Videovigilância

Solução de criptografia WaveLogic da Ciena

O WaveLogic Encryption oferece uma solução de criptografia óptica de alto desempenho e simples de implementar que se integra diretamente à rede de transporte. Com uma abordagem do tipo "configure e esqueça", a criptografia está sempre ativa (always on), garantindo o mais alto nível de segurança e eliminando erros humanos que possam resultar no envio de dados confidenciais não criptografados pela rede. Conforme mostrado na Figura 1, o WaveLogic Encryption garante que todos os dados e metadados críticos de serviços públicos que trafegam pela rede da concessionária estejam sempre seguros.

A solução é validada externamente e certificada de forma independente por terceiros para garantir que seja implementada usando algoritmos padrão do setor e recursos de segurança avançados. Ele fornece um mecanismo de criptografia AES-256 certificado por FIPS que inclui mecanismos de autenticação baseados em padrões (como certificados X.509), permitindo a integração perfeita em KPIs corporativos existentes, bem como suporte para os

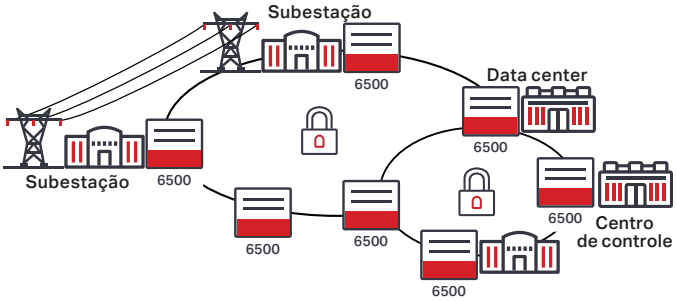

Figura 1. WaveLogic Encryption da Ciena

algoritmos de criptografia de chave pública mais recentes, incluindo criptografia de curva elíptica (ECC). Além disso, os componentes de hardware e software dos módulos criptográficos são compatíveis com FIPS 140-2, oferecendo a garantia de que a solução de criptografia está em conformidade com todos os aspectos abordados por essa avaliação abrangente, incluindo algoritmos de criptografia, mecanismos de troca de chaves e autenticação de usuário.

A solução de criptografia WaveLogic da Ciena permite às concessionárias:

- Convergir perfeitamente as redes de serviços públicos OT/TI e atender aos requisitos de conformidade em uma única infraestrutura convergente e altamente segura
- Estar em conformidade com os requisitos NERC-CIP para proteger redes de serviços públicos por meio de criptografia certificada FIPS de todos os dados em trânsito em tempo integral (24/7)
- Aproveitar as ofertas de largura de banda flexível com criptografia de alto desempenho e independente de protocolo de 10G, 100G ou 200G sem impacto no desempenho das aplicações das concessionárias
- Obter benefícios de uma abordagem de gerenciamento de criptografia simples e integrada que particiona o gerenciamento de criptografia do gerenciamento de transporte. Isso permite que a equipe de rede da organização de serviços públicos gerencie a rede enquanto a equipe de segurança mantém o controle total dos parâmetros de segurança de criptografia associados aos dados críticos da concessionária, emitindo novas chaves ou certificados conforme exigido por suas políticas de segurança

Solução WaveLogic Encryption
Baixe a nota sobre a aplicação

A criptografia de dados em repouso e em trânsito não é mutuamente exclusiva. Elas geralmente são implementadas em conjunto e se complementam como parte de uma estratégia de segurança holística. Ao implementar uma estratégia de segurança de dados profunda e em várias camadas, as concessionárias devem entender o caso de uso, a aplicação e os requisitos de conformidade. Além disso, o software ou tecnologia escolhida deve atender ao mais alto nível de padrões e algoritmos de criptografia. A solução de criptografia WaveLogic da Ciena combina um alto grau de flexibilidade e segurança com facilidade de operação e administração para permitir uma solução rentável, de criptografia de alto desempenho de latência ultrabaixa para o mercado de serviços públicos.

Faça suas perguntas na
Comunidade da Ciena