Eficiência na implementação de segurança de redes

Luis Lhullier, CTO na Nap IT – Global Network Solutions

Sistemas de segurança podem prejudicar a performance de um ambiente de rede se forem mal implementados. O ideal é que a implementação seja alinhada, do começo ao fim, com o time de TI e com o financeiro da empresa para que seja corretamente parametrizada, garantindo que os dados sensíveis ao negócio estejam bem protegidos e os sistemas de backoffice tenham o desempenho adequado para não comprometer a operação.

Atualmente, investimentos em cibersegurança estão no topo da torre de prioridades da área de TI das empresas. Isso acontece devido ao aumento exponencial de ataques e sequestros de dados realizados através de ransomwares. Os hackers têm não só derrubado os sistemas das empresas como sequestrado dados em troca de recompensa monetária para não expor dados corporativos sensíveis na Internet.

Mas apesar de necessária, a aplicação de sistemas de segurança pode prejudicar a performance de um ambiente de rede se as soluções forem mal implementadas. O ideal é que a implementação seja alinhada, do começo ao fim, com o time de TI e com o business para que seja corretamente parametrizada, garantindo que os dados sensíveis ao negócio estejam bem protegidos e os sistemas de backoffice tenham o desempenho adequado para não comprometer a operação.

Eficiência

Fora do cenário ideal, empresas que não possuem uma área de segurança, geralmente, buscam por soluções com o menor custo e o menor tempo de implantação. Caso o integrador busque um alinhamento no mesmo sentido, sem se preocupar em oferecer soluções mais adequadas às

necessidades do negócio do cliente, as tecnologias acabam sendo subdimensionadas ou mal parametrizadas.

Outra situação corriqueira é quando a empresa implementa um sistema de segurança e não tem um time de SOC - Security Operations Center para fazer atualizações. Como diversas ameaças são criadas e exploradas diariamente, o ritmo de defasagem de sistemas de segurança é muito rápido também.

É nesse contexto que o problema acaba sendo mascarado e o ambiente segue exposto e suscetível a ataques de ransomware, phishing e malware, que são os tipos de ameaças mais explorados e que, consequentemente, mais impactam os ambientes das empresas. Esses são os ataques mais comuns hoje em dia porque exploram o usuário como porta de entrada.

Durante a pandemia, quando os colaboradores saíram de dentro das empresas e foram trabalhar de casa, ficou muito mais fácil para os atacantes utilizarem os notebooks para implantar ameaças que são ativadas quando se conectam à rede corporativa.

A correta integração de sistemas certamente reduz a exposição a vulnerabilidades. Às vezes o simples fato de aplicar as melhores práticas na configuração de sistemas (que não são especificamente de segurança) já evita novos riscos.

Para citar um exemplo, um sistema de autenticação que não esteja configurado para permitir somente a conexão de sistemas consumidores acaba abrindo brecha para que a base de usuários da corporação fique exposta e possa ser explorada.

Um segundo exemplo muito interessante e muito visto no mercado é a segurança na codificação de sistemas. Um código mal implementado pode ser explorado por atacantes e expor facilmente dados financeiros e de cadastro de clientes.

Tendências

Voltando ao cenário do home office, a adoção de soluções baseadas em nuvem para força de trabalho remoto se tornou uma tendência. Conhecidas como Secure Remote Workforce, as soluções justamente endereçam as brechas em que colaboradores que atuam remotamente estão suscetíveis. Soluções de proxy, antimalware, antiransomware, que antes eram implementadas dentro da organização, foram adaptadas para reforçar a segurança nos dispositivos de usuários independentemente de onde eles estejam.

Apesar de as corporações terem conhecimento da existência dessas soluções, inclusive pelo apoio de portais e revistas especializadas, como a ***RTI***, que costumam apresentar as soluções e os serviços disponíveis no mercado, somente uma empresa especializada em segurança é capaz de auxiliar na identificação das tecnologias que melhor se adequam às necessidades de cada empresa. Esse processo se dá por meio

Acompanhe a série de *webinars RTI*

DISPONÍVEIS NO YouTube

rti WEBINAR | Experiências e aprendizados reunidos em um só canal

Apresentações com convidados selecionados para debater sobre normas, atualizações, regras e tendências do mercado!

INSCREVA-SE EM NOSSO CANAL
ACOMPANHE OS PRÓXIMOS EVENTOS

FEIRA E CONGRESSO 10ª EDIÇÃO NETCOM2022 INFRAESTRUTURA DE REDES TELECOM E PROVEDORES DE INTERNET

Agora você pode manter conexão com o mercado durante o ano todo!

Realização: aranda

Tel.: (11) 3824-5300
www.arandanet.com.br
YouTube

Promoção: rti REDES, TELECOM E INSTALAÇÕES

de dois passos essenciais: as conversas com o cliente e a análise do ambiente de rede (assessments de rede).

Com esse mapeamento é possível realizar uma prova de conceito (gratuitamente) para validar se a solução está realmente aderente às necessidades do cliente. A preocupação em entender esse aspecto, assim como o ambiente avaliado, antes de propor qualquer solução, é o que agrega valor aos projetos de segurança e garante sua eficiência.

Como profissional da área, posso afirmar que muitas vezes resolvemos os problemas com as soluções que o cliente possui em casa, reduzindo consideravelmente o custo com a aquisição de novos produtos sem reduzir o nível de segurança.

Por outro lado, é difícil dizer que todos os incidentes de segurança podem ser evitados, pois surgem novas ameaças que podem ser exploradas a todo momento.

As empresas que utilizam o SOC têm a seu favor um serviço de monitoramento da segurança que atua de forma preventiva. O SOC consiste em implementar sistemas (ou utilizar sistemas já implementados) para coletar informações sobre as diferentes soluções do cliente de forma centralizada e disponibilizar um time de especialistas para agir caso encontre ameaças, evitando e mitigando brechas de segurança.

Aí está a importância de se ter uma operação capaz de, ao ocorrer um incidente de segurança, agir para estancar o problema e trabalhar na resolução com agilidade e eficiência.

Conclusão

As empresas brasileiras ainda têm muito a evoluir dentro do campo da segurança. Mesmo com o crescimento dos investimentos das empresas nesse setor, ainda são valores irrisórios perto do que investem para manter a segurança de seus dados e dos dados dos clientes. Isso tem muito a ver com a rigidez com que as leis de proteção de dados são impostas no exterior.

Enquanto nosso mercado se ajusta, alguns pontos de atenção e de melhoria podem ser adotados como um caminho a ser seguido para as empresas protegerem seus dados:

• Para proteger um ambiente corretamente é preciso entender como ele está operando. Portanto, realize avaliações do ambiente atual.

• Procure uma empresa especializada para a definição das soluções a serem integradas e a forma como ela será entregue. Às vezes, ter uma solução casada com um serviço recorrente é a melhor opção para que as tecnologias atuem na melhor performance, entregando os melhores resultados.

• Defina como será realizado o monitoramento contínuo da segurança (interno ou por meio de SOC terceirizado), pois esse pode ser o ponto crucial para o ambiente se manter seguro.

www.klint.com.br

PROGRAMA
GREEN IT FURUKAWA.
A CONTRIBUIÇÃO DE SUA EMPRESA PARA UM MUNDO +SUSTENTÁVEL.

O Programa Green It Furukawa troca seus cabos de cobre de gerações anteriores, seja qual for o fabricante, por novos produtos Furukawa - cabos eletrônicos, de energia e de telefonia. O material substituído recebe tratamento especial e reciclagem, transformando-se em matéria-prima para indústrias, em novas aplicações, ajudando a proteger o planeta.

Redes sociais

5 PASSOS PARA UM DESCARTE CONSCIENTE

1 **Cliente** solicita o Progama.
2 **Furukawa** envia embalagens apropriadas.
3 **Cliente** envia o material e a nota fiscal da venda.
4 **Furukawa** recebe o material e envia o Cheque Verde.
5 **Cliente** recebe o Cheque Verde e solicita o Certificado.

DISTRIBUIDOR AUTORIZADO
FURUKAWA ELECTRIC
KLINT
Mais que conectividade!

Santo André - Matriz: Tel.: (11) 4972-9300 | Campinas: Tel: (19) 3773-9300
Bauru: Tel.: (14) 3103-0093 | Curitiba: Tel.: (41) 3262-9300
Rio de Janeiro: Tel.: (21) 3600-1555 | Espírito Santo: Tel.: (27) 3065-9300