Fator humano: o principal componente da segurança da informação

Vladimir Prestes (*)

A proteção de dados confidenciais nas empresas é baseada no componente técnico e no fator humano

De acordo com as últimas tendências de desenvolvimento da segurança da informação o foco passa a ser o indivíduo. Isto é evidenciado por tecnologias tais como: UEBA (User and Entity Behavior Analytics), UBA (User behavior analytics), SUBA (Security User Behavior Analytics) e outras ferramentas de análise de comportamento de usuários, que visam detectar ameaças presentes.

As ameaças em TI podem ser divididas em dois grandes grupos: tecnológicas e "humanas". Proteção antivírus, filtragem de tráfego, cobertura de vulnerabilidades, proteção contra ataques direcionados, DDOS – são tarefas com as quais soluções especializadas lidam de modo automático, já que a lógica do computador reconhece bem as ameaças e é capaz de tomar decisões sobre seu bloqueio autonomamente.

Ameaças "humanas" em TI – é uma área especifica. Contra elas não há uma solução totalmente automatizada. E geralmente essas ameaças são tratadas de forma integrada: configura-se o acesso aos componentes da infraestrutura de TI, utiliza-se sistema DLP (Data Loss Prevention), aumenta-se o conhecimento técnico dos funcionários e introduzem-se regulamentações de trabalho com informações críticas para os negócios.

As ameaças são muito distintas. Por isso, diferentes funcionários e até mesmo departamentos trabalham com elas: funcionários do departamento de TI cuidam das ameaças tecnológicas; profissionais de segurança da informação são responsáveis pelo monitoramento do "fator humano". A propósito, o departamento de TI nem sempre sabe quais as soluções e métodos de proteção estão sendo usados na empresa. Isso cria um tipo de contrapeso aos riscos que podem ser ocasionados pelos próprios profissionais TI. Em geral, essa abordagem mais precisa da segurança é praticada por empresas de médio e grande porte.

A proteção contra "ameaças humanas" possui um caráter integrado, ao mesmo tempo são aplicadas soluções especializadas e medidas administrativas.

Por um lado, é necessário elevar o nível de capacitação técnica de seus funcionários, de modo que informações confidenciais não venham a ser encontradas em e-mails pessoais, em anotações de smartphones ou, por descuido, não venham a cair nas mãos de terceiros. Representantes da empresa Cybersecurity Ventures, especializada em pesquisas no campo da segurança cibernética e análise de mercado, afirmam que os custos globais com treinamento de funcionários no âmbito da segurança da informação podem chegar a 10 bilhões de dólares até 2027.

Por outro lado, é importante acompanhar a movimentação de dados confidenciais que podem ser transmitidos para fora do "perímetro" da empresa. Apenas o uso integrado de soluções técnicas e medidas administrativas serão capazes de impedir a maioria dos vazamentos de informações. As consequências destrutivas provocadas por vazamentos são óbvias, mas os riscos causados pelo fator humano, muitas vezes, podem levar uma empresa à falência.

Na luta contra vazamentos de informações, todas as empresas estabelecem tarefas semelhantes: impedir o roubo de dados financeiros, evitar danos à reputação, manter em segredo assuntos internos, não perder a carteira de clientes, proteger os dados pessoais de funcionários e clientes. As ameaças tecnológicas podem interromper temporariamente o trabalho de uma empresa, as comunicações, o contato com os clientes - mas tudo isso é resolvido rapidamente. Em contrapartida, um alto executivo mal intencionado, possuindo acesso a todos os dados secretos, planos, documentos financeiros e analíticos, podendo causar não apenas sérios danos ao negócio, mas destruí-lo completamente.

A imprudência de um funcionário de um de nossos clientes resultou no vazamento de dados confidenciais. O gerente da empresa simplesmente esqueceu o notebook em cima da mesa da sala de conferências onde havia ocorrido uma reunião com um cliente. O notebook continha muitas informações interessantes: um arquivo com ofertas comerciais para o ramo de atuação do cliente, sistemas de formação de preços, arquivo de contratos, planos, etc. O sistema DLP registrou a tentativa de download dos documentos para uma mídia externa e um grande vazamento foi evitado. No entanto, o cliente acabou visualizando dados aos quais ele não deveria ter tido acesso.

E vazamentos ocasionais como estes não são raros. De acordo com uma pesquisa realizada pela SearchInform, em 2016 eles foram responsáveis por 42% de todos os incidentes relacionados à segurança da informação nas empresas dos países da CEI (Comunidade dos Estados Independentes).

Para garantir a proteção das informações da empresa é necessário desenvolver sua estratégia de segurança da informação ou seguir as recomendações abaixo, que permitem a redução de riscos:

1. Estabeleça regras para o manuseio de informações. A estrita observância das regras de armazenamento e operações com dados e documentos confidenciais diz respeito a qualquer funcionário - desde o mais alto executivo até o profissional comum.

2. Realize o treinamento dos funcionários do departamento de segurança da informação. Isso pode ser feito dentro da estrutura de sua organização: atribua esta tarefa ao departamento de RH ou de TI, ou inclua esta função às reponsabilidades do departamento de SI. Também é possível recorrer aos serviços de empresas especializadas em treinamento de agentes de segurança da informação (CTI, Security Awareness Training).

3. Crie o departamento de Segurança da Informação, que trabalhará na prevenção de incidentes. A tarefa dos funcionários de SI não é apenas investigar violações, mas analisar potenciais ameaças. Por exemplo, dar atenção especial aos funcionários que se enquadram em grupos de risco: apostadores, dependentes químicos, funcionários em processo de demissão ou insatisfeitos, etc.

4. Implemente soluções de proteção da informação. Use ferramentas de controle de informação: sistema DLP, sistema SIEM, etc. É necessário monitorar o maior número possível de canais de transmissão de informação dentro da empresa.

5. Abandone a abordagem convencional de proteção. Por si só, a implementação de ferramentas de proteção de informações não é uma garantia de segurança, ainda mais se forem usadas apenas diante de uma necessidade. Frequentemente, o incidente ocorre e só então, descobre-se que algo não foi configurado corretamente: um canal não estava sendo monitorado, um usuário teve acesso a informações que deveriam ser restritas, etc. Configure as ferramentas corretamente e monitore os canais de informação constantemente.

6. Faça uso do princípio de "freios e contrapesos". Não delegue toda a responsabilidade e poder apenas a uma pessoa: justamente com esse propósito é estabelecido o departamento de SI, para ser o "contrapeso" ao departamento de TI, que muitas vezes tem acesso às mais importantes informações confidenciais e possui conhecimento técnico suficiente para usá-las indevidamente.

(*) É Diretor Geral da SearchInform no Brasil, líder russa em sistemas de segurança da informação há mais de 20 anos. Com mais de dois mil clientes e cerca de 1.200.000 computadores protegidos, possui escritórios em 16 países.

A convergência das redes de TI e OT está trazendo riscos à sua organização?

Na nova economia digital, os dados e o que você faz com eles são fundamentais para o sucesso. Os consumidores e também os funcionários exigem acesso imediato a informações importantes que permitem resolver problemas, tomar decisões acertadas ou realizar transações. Mas essa é a parte da equação de dados que a maioria de nós consegue ver

John Maddison (*)

Para competir de forma eficaz no mercado digital atual e capitalizar com os dados coletados e processados, as organizações precisam responder rapidamente às mudanças do mercado e demandas dos consumidores, ajustar a produção, realinhar seus recursos e gerenciar sua infraestrutura. É por isso que quase três quartos de todas as organizações começaram a convergir sua infraestrutura de tecnologia da informação (TI) com suas redes de tecnologia operacional (OT) tradicionalmente isoladas.

A convergência das redes de TI e OT traz riscos

Porém, a convergência que possibilita novos modelos de negócios ágeis também traz novos riscos consideráveis, muitos dos quais pegam as organizações de surpresa. A maioria das violações da arquitetura de Controle e Aquisição de Dados e Sistemas de Controle Industrial (SCADA/ICS) causou um impacto alto ou significativo nos negócios, comprometendo a capacidade de atender aos requisitos de conformidade e diminuindo a funcionalidade e estabilidade financeira, além de afetar a segurança dos funcionários. Para as organizações de OT responsáveis pela infraestrutura crítica, qualquer tipo de impacto precisa ser levado a sério.

Estas são apenas algumas das descobertas de um novo estudo realizado pela Forrester Consulting, que analisa o estado atual da proteção da infraestrutura crítica, incluindo seus desafios, prioridades e estratégias relacionados. Este estudo, realizado em janeiro de 2018, entrevistou 429 tomadores de decisão globais responsáveis pela segurança da infraestrutura crítica, proteção IP, IoT e/ou sistemas SCADA.

- A maioria das organizações reconhece a importância da segurança SCADA/ICS e já realizou várias medidas para proteger seus sistemas SCADA/ICS, mas também planejam aumentar os gastos com segurança SCADA/ICS em 77%, mais do que em qualquer outro segmento de sua rede de TI ou OT. Parte do motivo deste aumento de investimento é que quase todos os tomadores de decisão reconhecem que há desafios de segurança muito graves relacionados à convergência de TI e OT.
- As principais preocupações de CSOs/CISOs incluem a incapacidade de identificar, medir e rastrear adequadamente os riscos, as interrupções nos sistemas que afetam os processos de cliente e nas operações de negócios causadas por uma catástrofe. Além disso, existe um número insuficiente de profissionais especializados em segurança, não apenas na própria equipe interna (40%), como também nos fornecedores de serviços de segurança terceirizados (41%). Isso não é apenas resultado da crescente lacuna de capacitação em cibersegurança em toda a indústria de computação, pois inclui o fato de que, mesmo entre os profissionais de segurança disponíveis, poucos têm experiência em ambientes de OT.
- Esse enfoque na segurança está sendo reforçado por uma série de problemas, sendo que o maior deles é a inclusão de soluções na nuvem a sistemas ICS, além da incapacidade de identificar ou agir no risco resultante da visibilidade e do controle limitados que a infraestrutura e os serviços na nuvem podem oferecer. Depois das preocupações com os ambientes na nuvem, os próximos cinco vetores de ataque à segurança SCADA/ICS que tiram o sono dos líderes de segurança em termos de ambientes de OT são: vírus (77%), hackers internos (73%) ou externos (70%), vazamento de informações confidenciais ou sensíveis (72%) e falta de autenticação do dispositivo (67%).
- Cada organização pesquisada agora possui tecnologias de IoT, uma média de 4,7 tipos diferentes de tecnologias de IoT conectada à rede de cada uma delas, incluindo RFID passivo, rastreamento de localização em tempo real (RFID ativo, banda ultralarga, ultrassom, etc.), rastreamento por GPS, sensores de segurança, sensores de rede e sensores de condição. Esses dispositivos também usam uma ampla variedade de protocolos de comunicação, incluindo Wi-Fi, sistemas celulares como CDMA/GPRS/4G, redes de malha, telemática e comunicações de campo próximo (NFC). Cada uma dessas tecnologias não apenas apresenta seus próprios desafios de segurança, mas como envolvem muitas questões de segurança inerentes aos dispositivos IoT que foram desenvolvidos com códigos ruins, que permitem invasão via backdoors e senhas embutidas diretamente em seu firmware ou que funcionam como dispositivos headless, impedindo até mesmo atualizações e correções básicas.

O que você pode fazer?

Para muitas organizações nessa mesma situação, uma dúvida muito comum é por onde começar. A maioria das organizações pesquisadas acha que a melhor maneira de evitar os desafios relacionados à OT e TI convergentes é fazer uma avaliação completa dos riscos operacionais e dos negócios, independentemente de estarem ou não na sua estratégia de convergência.

Outras medidas importantes que as organizações podem considerar, com base nas melhores práticas e no feedback dos participantes do estudo, incluem:

- Implementar controles essenciais de segurança de rede, como NGFW, IPS e sandboxing na borda do ambiente de OT; aumentar a centralização do gerenciamento de dispositivos e da tomada de decisões; criptografia de dados e tráfego; e considerando a natureza altamente sensível dos sensores e sistemas instalados nos ambientes de infraestrutura crítica, implementar monitoramento e controles passivos no ambiente de OT.
- Isolar a infraestrutura crítica das redes de produção, dispositivos de TI e dos funcionários usando estratégias de segmentação e microssegmentação.
- Fazer registros e análises contínuos de todo o tráfego de rede (análise de segurança).
- Usar autenticação de dois fatores, incluindo biometria (por exemplo, impressão digital, voz, reconhecimento facial, etc.) e estabelecimento de controle de acesso baseado na função para todos os funcionários via gerenciamento de identidade e acesso (IAM) e gerenciamento de identidades com privilégios (PIM) para administradores.
- Desenvolver internamente conhecimento sobre segurança específica dos sistemas SCADA/ICS, OT e IoT.

Problemas mais complexos exigem abordagens mais simples

O sucesso na nova economia digital exige o desenvolvimento de redes integradas capazes de utilizar todos os recursos disponíveis, seja dentro da rede de TI tradicional, por meio de dispositivos e aplicativos de usuários, em ambientes multinuvem, e até mesmo em sistemas SCADA/ICS na sua rede OT. Porém, isso traz novos riscos, muitos dos quais com consequências devastadoras. Com os ataques cada vez mais frequentes, a possibilidade de uma catástrofe colocar trabalhadores ou mesmo comunidades em risco continua aumentando; por isso, as organizações precisam tomar precauções que permitam ver e responder às ameaças, ou até mesmo antecipá-las, independente de onde elas possam ocorrer em toda a rede em expansão.

(*) É vice-presidente sênior de produtos e soluções da Fortinet.

Cinco dicas para micro e pequenos empresários driblarem imprevistos

De acordo com um estudo realizado pelo Instituto Brasileiro de Planejamento e Tributação (IBPT) e Empresômetro, a paralisação dos caminhoneiros em todo o país provocou um prejuízo estimado de mais de R$ 26 bilhões em negócios não realizados, considerando apenas os oito primeiros dias. Das microempresas às grandes corporações, de consumidores a fornecedores, todos os setores da economia sentiram o impacto.

A Intuit, multinacional que oferece soluções para controle financeiro de pequenas empresas e de pessoas que trabalham por conta própria, atende cerca de 4 milhões de pessoas no mundo com o QuickBooks, solução baseada na nuvem para planejamento e gestão de finanças que pode ser utilizada em PCs, tablets e smartphones.

Muitos dos micro e pequenos empresários de vários segmentos que utilizam o QuickBooks afirmaram que foram afetados pela greve de alguma forma, seja pelo cancelamento de reuniões, a queda nas vendas ou o atraso no recebimento de materiais.

"É necessário planejar inclusive os imprevistos, uma vez que para o microempresário é possível mudar a rota rapidamente", afirma Lars Leber, country manager da Intuit no Brasil.

Os micro e pequenos empresários podem aproveitar a sazonalidade da Copa do Mundo e do Dia dos Namorados para compensar os possíveis impactos da greve por meio de planejamento e proatividade. Confira as dicas para pequenos e médios empreendedores passarem por situações imprevisíveis e darem continuidade aos negócios:

1) Mantenha o fluxo de caixa para imprevistos e períodos de recessão;

2) Seja persistente e tenha paciência para passar pelos desafios diários dos negócios;

3) Aprenda a lidar com a própria ansiedade – faça um planejamento anual e procure manter sua atenção no cumprimento das metas a curto e médio prazo;

4) Seja proativo e faça a gestão de seus clientes para novos negócios;

5) Busque diversificar seus fornecedores – em caso de atraso ou parada repentina você não fica na dependência de um só fornecedor.

News @TI

Ainda dá tempo de se inscrever no programa Iguá Lab

@Empreendedores podem se inscrever até o dia 15 de junho no Iguá Lab, programa da Iguá Saneamento para seleção de startups. A companhia busca projetos com soluções para cinco desafios na área de saneamento: inadimplência, perdas de água, comunicação com clientes, treinamento de colaboradores e tecnologia. A iniciativa pioneira é promovida em parceria com o BrazilLAB e a Aceleradora Organica (www.igualab.com.br).