Empresas & Negócios

Matéria de capa

FREEPIK

CRIME CIBERNÉTICO ESTÁ EM CONSTANTE EVOLUÇÃO

CONSTRUINDO UMA PLATAFORMA SEGURA QUE AJUDA A COMBATER O CRIME CIBERNÉTICO

O ano de 2020 foi um alerta para todas as empresas que ainda estão atrasadas na curva digital. Como centenas de milhões de pessoas estão trabalhando em casa, nas circunstâncias sem precedentes causadas pela crise da COVID-19, as medidas de segurança cibernética foram estendida até o limite e os criminosos perceberam as oportunidades. Embora muitas empresas já tenham aproveitado as oportunidades trazidas pela transformação digital – Inteligência Artificial (IA), redes móveis sem fio de quinta geração (5G) e a crescente disponibilidade de energia computacional barata –, elas não são as únicas a colher os dividendos.

Os cibercriminosos estão utilizando da mesma tecnologia para seus próprios fins maliciosos - sejam ataques cibernéticos, fraude de dados, roubo ou todos os itens acima. Os ciberataques à infraestrutura crítica afetaram setores como os de energia, saúde e transporte. Enquanto isso, a mudança quase universal das organizações para um modelo de ecossistema - parcerias intrincadas e longas cadeias de suprimentos, possibilitadas pela computação em nuvem - colocou os setores público e privado em um maior risco de serem reféns dos cibercriminosos.

"Se olharmos para a COVID-19, há grandes semelhanças", diz Philipp Hurni, Líder de Prática Global em Engenharia de Riscos Cibernéticos da Zurich Insurance Group. E explica: "você precisa estar ciente de que ele existe e ter uma higiene específica para impedir que você o pegue. E, se você o contraiu, como se tratar e se recuperar? Isto é exatamente a mesma forma de como o ransomware está sendo espalhado - como vimos com o WannaCry e o NotPetya -, na medida em que há uma ampla gama de informações que você precisa conhecer para enfrentá-lo".

Além da pandemia, que virou a vida das pessoas de cabeça para baixo este ano, há outros paralelos entre os riscos tradicionais - como incêndio e inundação - e a maneira como o ransomware afeta os negócios. "Incêndios e inundações não se importam se causam danos ou não, enquanto um cibercriminoso se adaptará a isso", afirma Hurni.

"As empresas têm seu seguro contra incêndio e responsabilidade civil, mas o seguro cibernético precisa estar próximo disso, porque esses desastres podem ser verdadeiramente catastróficos para o seu negócio", acrescenta.

Segundo o executivo, todo mundo sabe que uma fábrica em chamas significa uma grande perda, porque atrapalha a produção

FREEPIK

comercial. Porém, nem todo executivo entende que os problemas cibernéticos podem ser ainda mais desastrosos, pois podem afetar muitos locais diferentes ao mesmo tempo. "A ameaça de crime cibernético é, de muitas maneiras, ainda maior por estar em constante evolução. Incêndios e inundações não se importam se causam danos ou não, enquanto se um criminoso cibernético não for bem-sucedido, ele se adaptará e voltará a atacar com técnicas diferentes", diz.

No entanto, aderir aos modelos tradicionais herdados da tecnologia da informação (TI) - desenvolvidos internamente e de forma mais fácil, protegidos contra riscos externos - não é mais viável para os negócios modernos. Mais de 75% dos líderes empresariais acreditam que os ecossistemas serão os principais disruptores dos modelos de negócios nos próximos cinco anos. O risco pode ser gerenciado com sucesso, no entanto. O ponto de partida é reconhecer que cada empresa agora possui um grande "fator de dependência de tecnologia da informação".

FREEPIK

Isso inclui os provedores de nuvem nos quais os aplicativos comerciais estão sendo executados, funções comerciais terceirizadas, como ferramentas de gerenciamento de RH ou processadores de pagamento e a cadeia de suprimento físico automatizada, cada vez mais direcionada por TI, de matérias-primas e peças. Embora o perigo representado por esse admirável mundo digital seja real e evidente, ele tem sido um risco "crescente", aumentando ano após ano, com as etapas da cadeia de valor cada vez mais se tornando digitais.

A maioria das empresas raramente conhecem totalmente o aumento do risco cibernético e, portanto, negligenciaram tomar contramedidas. "Isso precisa mudar", diz Hurni. "Primeiro, você precisa criar uma estrutura formal e recursos dedicados para identificar e gerenciar o risco. Também é necessário criar uma cultura de alfabetização digital em seus negócios e cadeia de suprimentos, para que todos entendam como o risco digital funciona para os ecossistemas. É preciso aprender e ensinar sempre, porque os cibercriminosos estão se tornando especialistas em engenharia social, espionando ecossistemas inteiros e, depois, invadindo uma organização para lançar um ataque ainda maior".

"Mesmo assim, algumas pessoas ainda clicarão em um link de malware e eles infectarão sua máquina. Portanto, é necessário haver um sistema de monitoramento constante, com pessoas e processos para detectar violações e reagir rapidamente - porque você pode conter a severidade de um ataque cibernético drasticamente usando de resposta e recuperação rápidas", afirma.

O mesmo nível de vigilância é necessário em todo o ecossistema, com medidas tomadas para garantir que fornecedores e parceiros mantenham sua própria "higiene digital". Essa tensão contínua entre empresas e cibercriminosos só vai aumentar. Os ataques de ransomware - facilmente a maior ameaça cibernética hoje em dia - aumentaram 41% no ano passado. No entanto, a probabilidade de ser condenado por esses crimes é muito baixa.

E, longe de ser uma reserva de especialistas em computação altamente inteligentes e instruídos, essa forma de crime organizado está aberta a qualquer pessoa. "Anos atrás, você precisava ter um entendimento completo da tecnologia da informação para realizar ciberataques", diz Oliver Delvos, Gerente global de subscrição cibernética da Zurich.

"Mas, hoje em dia, os criminosos podem terceirizar o ransomware como um serviço da mesma forma que as empresas legítimas usam o Software como Serviço (SaaS). Os profissionais do ramo de crimes cibernéticos lidam com muitas tarefas individuais necessárias para realizar um ataque cibernético, fornecendo o malware e as listas de possíveis vítimas. Um ecossistema criminal foi criado com qualidade e profissionalismo amplamente aprimorados e, como o pagamento é feito com criptomoedas, os criminosos podem permanecer completamente anônimos".

"Você quase não precisa de nenhum conhecimento ou experiência para ser um cibercriminoso de sucesso - você pode basicamente ficar como apoio e usar as ferramentas fornecidas por eles", acrescenta Delvos.

Este é apenas o começo. O Relatório Global de Riscos 2020, produzido pelo Fórum Econômico Mundial em colaboração com a Zurich, classifica os ataques cibernéticos como o segundo risco mais preocupante para as empresas globais na próxima década.

Atualmente, já vemos métodos de inteligência artificial aplicados em técnicas de ataques cibernéticos - mas eles ainda estão começando. Na próxima década, essas tecnologias amadurecerão e o desenvolvimento da computação quântica poderá permitir que os cibercriminosos quebrem a maior parte da criptografia de ponta atualmente em um futuro não muito distante. Portanto, é obvio que o problema cibernético se tornará bem mais complexo e desafiador.

O tempo para agir e implementar um contraplano abrangente está efetivamente sobre nós. Principais tópicos:

- O risco cibernético é maior do que nunca - e cresce exponencialmente
- A transformação digital é uma força para o bem e para o mal
- Muitas empresas subestimam o risco cibernético
- As contramedidas precisam ser abrangentes, multifacetadas e apoiadas com financiamento e apoio da diretoria

Fonte e mais informações: (www.zurich.com.br).