A dimensão cibernética do coronavírus

Março de 2020

Observações

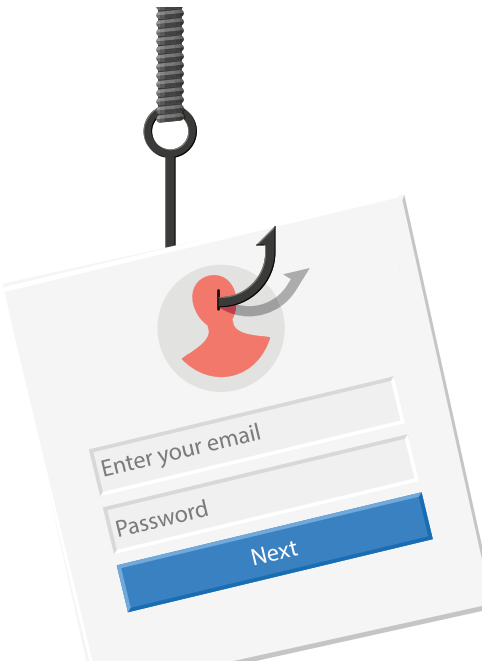
Nas últimas semanas, houve um aumento drástico no número de incidentes cibernéticos em empresas em todo o mundo, afetadas por uma nova onda de ataques cibernéticos relacionados ao coronavírus. Segundo a empresa de cibersegurança CYE, desde o início de fevereiro, cibercriminosos se aproveitaram cada vez mais da ignorância sobre a situação causada por essa pandemia global. A CYE observou um aumento cinco vezes maior de incidentes cibernéticos, principalmente na Europa.

Com o medo e o aumento da distração do público associada a esse evento, há uma probabilidade maior de os funcionários clicarem em arquivos maliciosos ou usarem redes não seguras para recuperar informações confidenciais quando estiverem trabalhando em casa ou em locais remotos. Conforme as quarentenas se tornam mais frequentes e cada vez mais pessoas são autorizadas a trabalhar remotamente, as empresas devem adotar uma abordagem multidepartamental para manter os nível de controle adequado.

De acordo com estudos recentes, campanhas de phishing e ataques de ransomware tiveram o maior aumento nas últimas semanas, conforme os usuários clicavam em arquivos ou links maliciosos sobre o coronavírus.

Houve recentemente um ataque sofisticado em que os cibercriminosos se apresentaram como funcionários da Organização Mundial da Saúde (OMS) e solicitaram informações confidenciais para distribuir um anexo que roubava informações pessoais.

Figura 1: Captura de tela de um e-mail de phishing fingindo ser da Organização Mundial da Saúde - Fonte: Proofpoint Inc



1 https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/amp/

Aumento dos riscos cibernéticos

O trabalho remoto e descentralizado aumenta o risco de ocorrência dos seguintes tipos de ataques:

Phishing/Spear phishing/Comunicações Fraudulentas: e-mails ou outras comunicações eletrônicas com informações específicas sobre o destinatário para induzi-lo a clicar em um link fraudulento, abrir um anexo malicioso ou tomar outras ações comprometedoras.

Business Email Compromise (BEC): e-mails direcionados aos destinatários para fazer transferências eletrônicas, geralmente representando o CEO, o CFO ou outros diretores da empresa.

Engenharia social: manipulação psicológica de pessoas para que ajam como normalmente não agiriam.

Esses eventos podem levar a um maior risco de ransomware, o que pode não apenas infectar e bloquear as redes de computadores das empresas e de seus clientes, como também criptografar ou destruir dados. Sabendo que alguns ataques cibernéticos podem permanecer inativos por dias, meses ou até anos, as ações tomadas hoje podem ter um impacto significativo na receita e na imagem de uma empresa no futuro. Felizmente, existem medidas preventivas que empresas e funcionários podem tomar para evitar esses eventos e manter um ambiente digital seguro e protegido.

Recomendações para mitigar riscos

Indivíduos:

Links/anexos: Não clique em links nem abra anexos de e-mails de remetentes não confiáveis. Se os funcionários quiserem navegar em um site, recomendamos escrever diretamente o URL do site que desejam acessar. Um URL seguro começará com https, e não http, mas esse critério não é suficiente: examine cuidadosamente o URL antes de digitar para verificar se ele aponta para o site oficial da empresa/instituição que você está tentando acessar. Em caso de dúvida, use um verificador de URL on-line, como o **isitphishing.org**, antes de acessar.

Informações: Não responda ou dê informações de nenhum tipo de conta a fontes desconhecidas. As entidades de confiança, como provedores ou vendedores, geralmente já possuem essa informação. Nunca envie informações de identificação pessoal e/ou senhas por e-mail para pessoas desconhecidas ou abra anexos em e-mails não solicitados.

Denuncie atividades suspeitas: Todos os e-mails suspeitos devem ser comunicados à equipe de segurança cibernética da empresa ou departamento equivalente.

Notifique o Suporte: Os funcionários devem entrar em contato com o Suporte local caso acreditem que abriram um anexo ou clicaram em um link que possa ter infectado o computador com um vírus ou malware.

Empresas:

Treinamentos de conscientização de funcionários/usuários: Antes de autorizar conexões remotas à rede corporativa, os funcionários devem ser devidamente treinados sobre campanhas de phishing e diretrizes de segurança e informados sobre todos os processos e procedimentos corporativos de denuncia ou notificação de um incidente de segurança em caso de suspeita ou identificação de uma possível violação de segurança ou privacidade.

Conexões seguras: Use apenas acesso remoto seguro às redes informáticas da empresa. Sempre que possível, por meio de uma rede virtual privada (VPN) ou outro mecanismo de conexão criptografada.

Autenticação multifatorial (MFA): As VPNs devem ser configuradas com autenticação multifatorial como uma camada adicional de segurança para garantir que apenas pessoas autorizadas acessem a rede corporativa.

Administração de dispositivos móveis (MDM): Os computadores, tablets e smartphones dos funcionários devem estar equipados com uma solução corporativa em MDM. A solução deve implementar controles apropriados de segurança e criar um ambiente virtual criptografado no dispositivo para armazenar e processar informações corporativas, por exemplo, documentos e e-mails.

Proteção do perímetro da internet: Os departamentos de TI devem garantir que os firewalls estejam configurados corretamente e monitorar o registro para identificar tentativas de conexão ou conexões bem-sucedidas de endereços de Protocolo da Internet (IP) não autorizados ou suspeitos.

Segurança na nuvem e conformidade: As empresas que usam serviços em nuvem devem garantir que as configurações de segurança sejam aplicadas e monitoradas adequadamente para identificar desvios ou alterações na configuração ou adulteração não autorizada.

Maior supervisão e diligência: Em caso de regiões ou países em que os funcionários não tenham motivos para se conectar remotamente à rede da empresa, o departamento de TI deverá colocar proativamente os intervalos de IP na lista negra (“blacklist”) dessas áreas para que não possam se conectar remotamente às redes corporativas.

Considerações finais

É natural se concentrar no que percebemos. A COVID-19 nos lembra de que o invisível e o intangível podem ter um impacto muito mais sério do que alguns dos riscos mais tangíveis que percebemos e nos informamos todos os dias (por exemplo: incêndios, roubos ou acidentes de trânsito). Os riscos cibernéticos, bem como a COVID-19, se enquadram nessa categoria de riscos intangíveis. Nos últimos anos, vimos vários eventos em que vírus digitais infectaram um computador atrás do outro e se tornaram uma verdadeira pandemia em um curto período. O incidente NotPetya em 2017 foi a maior dessas pandemias até o momento, afetando milhares de empresas em todo o mundo e causando uma perda econômica estimada em US$ 10 trilhões. Como acontece atualmente, a higiene é essencial para evitar qualquer infecção em primeiro lugar. Corrigir sistemas e lavar as mãos são igualmente importantes. Isolamentos de processos e/ou ambientes isolados ("Sandboxing") e quarentenas são incrivelmente semelhantes quando se trata do tratamento de uma possível contaminação.

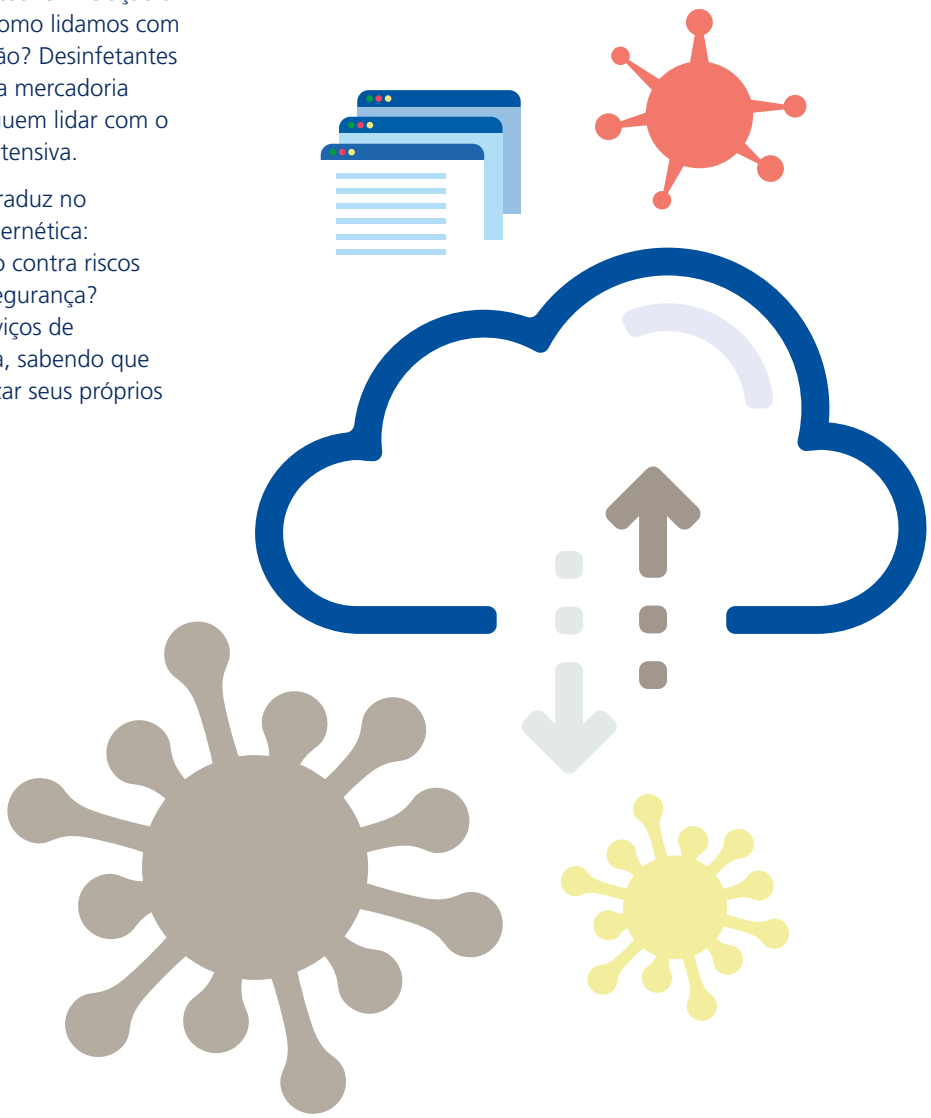
Quanto aos riscos cibernéticos, o Instituto Nacional de Padrões e Tecnologia (NIST) fornece uma estrutura para as empresas desenvolverem suas capacidades para identificar riscos cibernéticos, proteger, detectar, responder e se recuperar de ataques cibernéticos. Esses recursos incluem, mas não se limitam à tecnologia. Conforme descrito acima, a conscientização e os procedimentos constituem o núcleo de proteção. Uma detecção rápida e confiável, seguida, se necessário, pela resposta e recuperação adequadas é essencial. A situação atual em relação à COVID-19 também nos dá as seguintes ideias: Como lidamos com os aumentos repentinos na demanda por proteção? Desinfetantes para as mãos e máscaras faciais tornaram-se uma mercadoria escassa e centros e equipes de saúde mal conseguem lidar com o aumento de pacientes em unidades de terapia intensiva.

Portanto, devemos nos perguntar como isso se traduz no ambiente cibernético e na próxima pandemia cibernética: Podemos confiar em nossos recursos de proteção contra riscos cibernéticos e de resposta a incidentes de cibersegurança? Podemos confiar em provedores externos de serviços de tecnologia no caso de uma pandemia cibernética, sabendo que eles atendem a muitos clientes e precisam priorizar seus próprios recursos escassos?

Nossos recursos corporativos internos de segurança informática e de resposta a emergência são autossuficientes?

Por fim, a COVID-19 nos mostrou a complexidade das cadeias de suprimento e nossas dependências de bens intermediários de outros países e continentes. Atualmente, isso vale não apenas para provedores físicos, mas também para provedores de capacidade informática, armazenamento de dados e plataformas onde os aplicativos operam.

Nas últimas décadas, uma grande tendência na fabricação tem sido a terceirização, seguida pela descentralização dos serviços. Na tecnologia da informação, não foi diferente. Hoje, a migração para a nuvem é o próximo passo, e muitas empresas estão migrando suas infraestruturas de TI para a nuvem de grandes provedores de serviços. A oportunidade técnica de trabalhar com mais eficiência por meio de serviços na nuvem nos ajuda a responder e recuperar de um evento real de pandemia, mas também cria, consequentemente, uma vulnerabilidade intangível e invisível. Enquanto ainda procuramos um "botão de emergência" para a COVID-19, podemos refletir sobre o que esse vírus nos diz sobre nossos recursos de resiliência digital e segurança cibernética e como devemos nos preparar para o próximo vírus de uma epidemia cibernética.



Zurich Insurance Group

173006686 (03/20) TCL

ZURICH®