HACK3R_
RANGER5

SEGURANÇA CIBERNÉTICA NA ERA DA DEPENDÊNCIA TECNOLÓGICA

O mundo está viciado — e não, nós não estamos falando de substâncias psicoativas ilegais. Estamos falando da tecnologia. Todos os setores da sociedade (usuários finais, empresas e governos) estão marchando para um futuro no qual somos cada vez mais dependentes de inovações tecnológicas. A cada dia, surgem diferentes soluções, ferramentas e protocolos rumo à nova era de uma internet descentralizada.

O apetite pela adoção de conceitos como inteligência artificial (I.A.), Internet das Coisas (IoT), computação de borda, blockchain e 5G só tem aumentado diariamente. É claro, parte da culpa dessa digitalização desenfreada pode ser atribuída à acelerada transformação digital causada pela pandemia do novo coronavírus (SARS-CoV2). A crise impulsionou o trabalho remoto e a adoção de novos modelos de negócio que respeitassem o distanciamento social e permitissem um maior compartilhamento de dados entre múltiplos ambientes.

E as inovações não param: já estamos falando do metaverso e de um possível futuro no qual podemos passar mais tempo em um ambiente digitalizado do que no mundo real. Esse futuro conta com sua própria economia, baseada em criptomoedas e tokens não fungíveis (NFT), causando disrupções sem precedentes nas experiências socioeconômicas, além de uma imersão virtual jamais vista anteriormente. Porém, com o aumento da dependência tecnológica, como fica a segurança cibernética?

HACK3R_
RANGERS

O outro lado da moeda

Aumentos nos ataques cibernéticos

Naturalmente, todas essas inovações também aumentam a superfície de ataque. De fato, as estatísticas não mentem: a maior dependência de sistemas digitais cada vez mais complexos está reduzindo a nossa capacidade de responder às ameaças cibernéticas. Basta lembrar que, em 2020, nada menos do que US$ 406 milhões foram transferidos para as carteiras de criptomoedas de ransomwares — um valor quatro vezes maior em comparação com o ano anterior, no qual foi registrada uma movimentação de "apenas" US$ 93 milhões.

Não é à toa. Se as inovações tecnológicas causam facilidades em nossa vida, elas também podem ser usadas pelos cibercriminosos. Um "modelo de negócio" que já se provou rentável é o ransomware-como-serviço (ransomware-as-a-service ou RaaS), que permite que até mesmo uma pessoa sem qualquer conhecimento técnico licencie um malware para disparar um ataque de sequestro digital contra uma empresa. Os lucros são divididos com os operadores e a vítima fica a ver navios.

Os ransomwares também estão cada vez mais agressivos e alvejando pontos fracos. Mais do que simplesmente criptografar arquivos, eles passaram a praticar a dupla ou até a tripla extorsão, ameaçando divulgar os dados comprometidos ou aplicar ataques DDoS contra o servidor vitimado. Além disso, os alvos mais comuns se tornaram infraestruturas críticas, que não podem deixar de operar por uma hora sequer. Dessa forma, a pressão para o pagamento do resgate é ainda maior.

HACK3R_
RANGER5

Claro, os sequestros digitais não são as únicas ameaças que surgem com a maior dependência tecnológica. Nunca se falou tanto de ataques contra a cadeia de suprimentos, e há um porquê: ela também foi digitalizada. Confiamos cada vez mais em parceiros tecnológicos para garantir a correta operação das empresas, o que acaba criando situações delicadas, como a infecção em massa do plugin Orion, da SolarWinds, em 2020.

Além disso, quando foi descoberto o conjunto de vulnerabilidades no Log4j — biblioteca de código aberto usada por milhares de aplicações ao redor do mundo —, analistas registraram mais de 100 tentativas de ataque por segundo. O cibercrime percebeu que, no fim das contas, é mais fácil envenenar a fonte da água do que envenenar cada copo individualmente — e a necessidade de uma interoperabilidade cada vez maior entre sistemas faz com que o veneno se espalhe com uma velocidade estonteante.

HACK3R_
RANGERS

Preocupações futuras

No que devemos focar?

Na pesquisa Global Risks Perception Survey (GRPS), os participantes classificaram a “falha de cibersegurança” como um dos dez riscos que mais se agravaram após a crise da COVID-19. Além disso, 85% da Comunidade de Liderança do Fórum Econômico Mundial (World Economic Forum ou WHF) considerou o ransomware como a ameaça em crescimento que mais representa perigos para a segurança pública.

Para piorar a situação, temos o tão comentado apagão de talentos. Estima-se que sejam necessários mais de 3 milhões de profissionais de cibersegurança a nível global para prover respostas rápidas às ameaças, proteger sistemas e conscientizar os internautas sobre boas práticas de higiene cibernética. Fraudes e campanhas de desinformação também apresentam crescimentos preocupantes, com o uso de deepfakes para tornar os golpes ainda mais realistas.

E engana-se quem pensa que a situação não pode piorar: calcula-se que 40% da população global ainda não está conectada à internet. Essa parcela, que já está sofrendo com a iniquidade de direitos, se tornará uma comunidade ainda mais enfraquecida contra as ameaças virtuais emergentes de uma internet descentralizada e de uma economia altamente digitalizada.

HACK3R_
RANGERS

Resoluções para uma sociedade mais segura

Estatísticas também mostram que as empresas estão operando em um cenário no qual 95% dos problemas de cibersegurança podem ser considerados frutos de erro humano e 43% dos vazamentos são causados — intencionalmente ou não — por insiders.

Conforme nossa dependência tecnológica aumenta, é crucial que todos os participantes desse ecossistema trabalhem em conjunto para definir normas e regras de comportamento que garantam a segurança da nova web 3.0. Para mitigar os riscos, faz-se necessária uma maior cooperação entre as organizações, tanto para compartilhar inteligência contra ameaças quanto para trabalhar em iniciativas com foco nas novas tendências — como blockchain, computação quântica, I.A. e metaverso.

Dentro das corporações, um diálogo mais aberto entre os diferentes departamentos e um maior envolvimento da alta diretoria (board e c-levels) é essencial para otimizarmos nossas estratégias de segurança. Só assim caminharemos para um futuro com menor fragmentação e maior resiliência nos sistemas tecnológicos, que, inevitavelmente, estarão cada vez mais presentes em nossas vidas.

TESTE A NOSSA PLATAFORMA
GRATUITAMENTE DURANTE 15 DIAS!

HACKERRANGERS.COM

HACK3R_
RANGERS

Bibliografia
The Global Risks Report 2022 (World Economic Forum, janeiro de 2022)