TENDÊNCIAS DE CURTO E MÉDIO PRAZO PARA A SEGURANÇA DIGITAL

ED. 2022

O e-book traz um compilado de visões de organizações, respeitadas no mundo inteiro, sobre as previsões de curto e médio prazo para o segmento de segurança da informação. O material caracteriza leitura essencial para analistas e gestores de tecnologia que possuem interesse em manter suas estratégias de segurança aderentes aos movimentos de mercado.

ostec
Segurança digital de resultados

ÍNDICE

INTRODUÇÃO

Conforme 2021 chega ao fim, ficam mais precisas as previsões para esse mercado em 2022. Também já é possível adiantar, com um considerável grau de confiabilidade, algumas tendências que se desenham para os próximos cinco anos. Algumas delas já são bem palpáveis, enquanto outras seguem bastante incipientes. Em todas, porém, há fortes argumentos que mostram sua viabilidade, tornando-lhes dignas de ao menos uma leitura atenciosa e instrutiva.

É importante lembrar que segurança cibernética diz respeito a todos, pois estamos todos sujeitos a ser vítimas de phishing, ransomware e outros golpes, que estão cada vez mais sofisticados. Empresas precisam estar atentas, verificar se seus funcionários, parceiros e clientes têm conhecimento sobre cibersegurança para proteger seus ativos mais valiosos.

Monitorar a inteligência atual sobre ciberataques e táticas de proteção é fundamental para estar por dentro do que está acontecendo e garantir sua segurança.

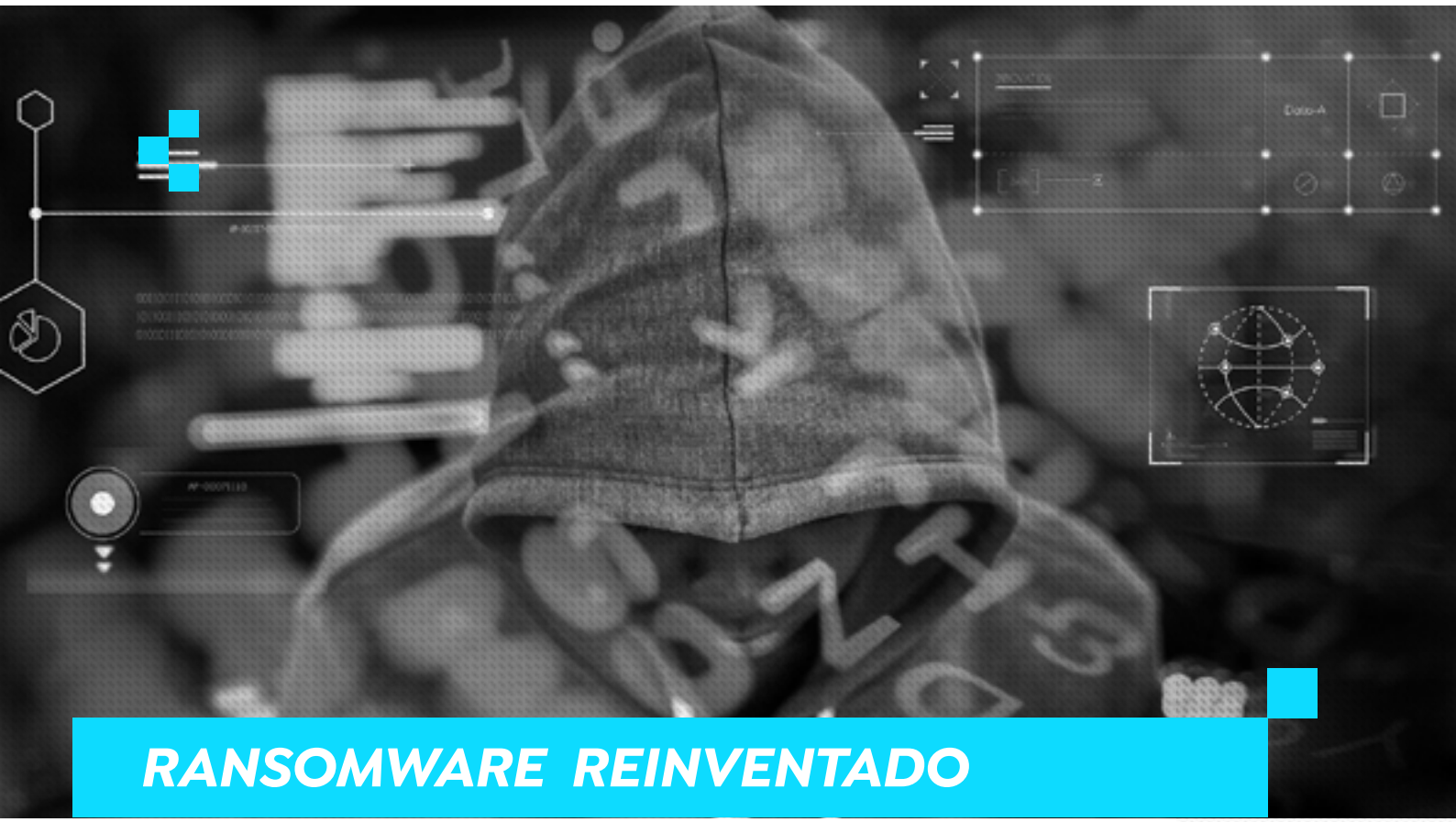
Portanto, separamos neste e-book tendencias de segurança digital que você precisa conhecer, e como elas estão remodelando a privacidade e a segurança da Tecnologia da Informação na Internet.

Boa leitura!

FALTA DE PROFISSIONAIS EM SEGURANÇA DIGITAL

A tendência é que 2022 seja um ano desafiador em relação à escassez de talentos para a segurança cibernética. Alguns impulsionadores desse desequilíbrio incluem a adoção acelerada de nuvem híbrida e iniciativas de transformação digital, projetos pós-pandemia aumentando e maiores orçamentos disponíveis. Assim, as melhorias nas abordagens de segurança estarão no topo da lista de projetos desejados, mantendo muitos profissionais nas empresas em que já estão – e até mesmo assumindo um segundo emprego.

Negócios, empresas, fornecedores de soluções, parceiros, provedores de serviços e muitos mais verticais alinhados à segurança digital sofrem na hora de contratar. As faculdades e universidades não estão produzindo profissionais de segurança na velocidade desejada, e o setor tem um alto grau de empreendedorismo – talentos que poderiam ser bons funcionários acabam criando as próprias empresas, reduzindo a oferta de trabalhadores. Assim, esse desequilíbrio causará picos salariais em todos os níveis de profissionais de segurança de TI.



RANSOMWARE REINVENTADO

O ano que está chegando ao fim viu o modelo de ransomware evoluir para incluir a extorsão de dados com base em informações exfiltradas. O problema é que isso ainda não acabou. Pelo contrário; novas maneiras de extorquir dinheiro surgirão em 2022.

Os gestores devem esperar que o ransomware se torne personalizado e envolva cada vez mais tipos de ativos, como IoT e membros internos da empresa. Nesse contexto, a divulgação direcionada de informações exfiltradas pode ser perpetrada para compradores específicos. Pode-se esperar até a chegada de termos de pagamento mais flexíveis; com os planos de parcelamento, os operadores de ransomware irão descriptografar os ativos da vítima ao longo do tempo, com base nos termos de pagamento acordados.

SEGURO CIBERNÉTICO EM RISCO

Nos últimos anos, o seguro cibernético se tornou comum no gerenciamento de riscos corporativos. Contudo, ataques de ransomware e outras falhas de violação colocaram esse modelo de negócio em risco. Posteriormente, muitas seguradoras cibernéticas aumentaram drasticamente as taxas, abandonaram a cobertura de empresas de alto risco de segurança ou até mesmo saíram completamente do mercado de seguros cibernéticos.

Em 2022, pode-se esperar muitos cancelamentos de seguros do tipo, bem como uma corrida desenfreada para obter novas coberturas – provavelmente com taxas muito mais altas. Para obter a melhor cobertura e garantir os preços mais adequados, as empresas precisarão criar os ambientes de segurança cibernética exigidos pelos corretores de seguro cibernético. O não acordo quanto aos controles de segurança também será um argumento importante para as seguradoras recusarem o pagamento após um incidente – ou encerrarem a cobertura.

LIBERDADE NAS REDES SOCIAIS

As redes sociais estarão sob pressão crescente para controlar o conteúdo postado por seus usuários. É provável que isso também resulte em poderes mais amplos para as autoridades rastrearem e identificarem fontes maliciosas.

O anonimato da rede permite que os usuários se escondam atrás dessas plataformas sociais, usando-as para espalhar fake news e adotarem um comportamento abusivo com relativa impunidade.

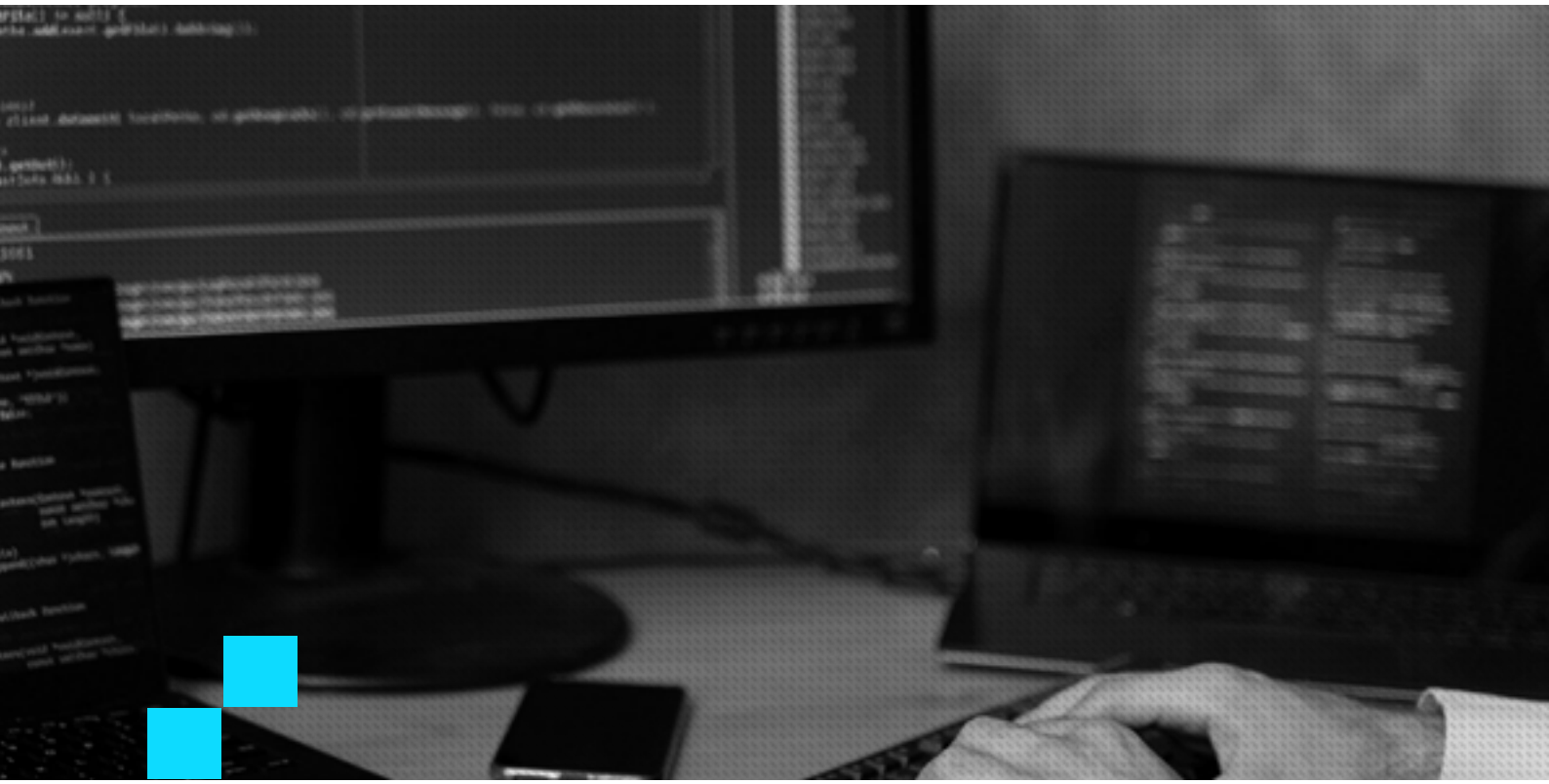
No próximo ano, haverá controles mais rígidos sobre o conteúdo que é distribuído por meio de plataformas sociais, com comprovação de fonte confiável e talvez até acesso aos dados por parte das autoridades.

DETECÇÃO DE INTRUSÃO MAIS DIFÍCIL

Em 2022, o tempo médio entre a intrusão e a detecção crescerá, dando aos invasores mais tempo para realizar o reconhecimento e causar estragos nos sistemas.

Assim, muitas empresas aceleraram as implementações de trabalho remoto com base na tecnologia VPN. Este é um dos fatores que contribuíram para tornar a detecção de intrusão mais difícil. As equipes enfrentam uma quantidade de dados muito maior para vasculhar e tentar distinguir o comportamento legítimo da atividade maliciosa.

Pode-se esperar muitos cibercriminosos que cuidadosamente encontrarão um caminho para entrar nos sistemas e se estabelecerem lá por muito tempo.



EVOLUÇÃO DE CIBERATAQUES

A cadeia de ataque normalmente é composta de etapas como exploração da vulnerabilidade, obtenção de acesso privilegiado, movimento lateral e exfiltração de dados ou danos operacionais. Em 2022, o número de ataques bem-sucedidos continuará a crescer, os danos para a vítima aumentarão e o padrão se repetirá. Afinal, com tantas tecnologias novas, os conceitos básicos de segurança de TI simplesmente não são adotados na mesma velocidade que as investidas dos cibercriminosos.

PARALIZAÇÃO DA INTERNET CAUSADA POR GRANDES EVENTOS

Seja por conta de um terremoto, guerra ou outro desastre natural – ou danos de proporções gigantescas causados pelo homem – a comunidade de tecnologia da informação pode não estar preparada o suficiente para uma paralisação massiva e prolongada.

À medida que os funcionários continuam a trabalhar em casa e a dependência da interconectividade aumenta, uma grande indisponibilidade ou perda de dados seria um divisor de águas para a tecnologia.

Seja por conta da consequência de um ataque cibernético imenso, uma pandemia ou um desastre natural induzido pelas mudanças climáticas, o mundo enfrentará sua primeira paralisação de longo prazo da Internet. Se na pandemia de Covid-19 a internet se tornou ainda mais essencial, imagine não poder contar com essa ferramenta caso surja um novo evento de proporções semelhantes.

O NOVO 'LIXO ESPACIAL'

Muitos especialistas presumem que os dispositivos 5G e IoT são naturalmente seguros. A realidade é que esses terminais costumam ser afetados por problemas como credenciais padrão, software sem patch ou vulnerabilidades de hardware, à medida que os fabricantes procuram produzir dispositivos de baixo custo em grande escala.

Um problema emergente nos próximos anos será como esses dispositivos IoT legados são mantidos e suportados. Assim como os detritos espaciais causam problemas para novos satélites, projetos de IoT abandonados e sistemas sem suporte serão alvos ideais para invasores. Uma vez que um cibercriminoso tenha uma posição segura dentro do sistema, ele pode construir uma infraestrutura distribuída para coletar dados ou lançar ataques altamente distribuídos, que podem ser amplificados por uma conectividade 5G mais rápida.

FUTURO SEM SENHA

Essa previsão renasce a cada ano com novas perspectivas. Existe um consenso quase universal de que as senhas são terríveis de se memorizar. Os humanos não são programados para gerar e lembrar combinações únicas e complexas de caracteres que não se parecem com nenhuma linguagem falada.

Ao longo dos anos, viu-se tentativas variadas de resolver o problema. Contudo, mais recentemente, o conceito sem senha parece estar finalmente ganhando força. Aplicativos de autenticação, Windows Hello e soluções SSO estão todos reduzindo a necessidade de passwords. Recentemente, a Microsoft permitiu que os usuários não usassem senhas usando o aplicativo Authenticator. Com menos pontos de acesso controlados por senhas, os invasores se concentrarão cada vez mais na exploração de usuários e aplicativos para obter acesso a dados e privilégios.

CONSCIENTIZAÇÃO DE USUÁRIOS E ATAQUES DE PHISHING DIRECIONADOS

Conforme as ameaças cibernéticas se tornam mais agressivas, as empresas tomam medidas para fortalecer suas defesas. Assim, a conscientização sobre a segurança digital é essencial para evitar invasões que podem destruir a reputação da companhia.

Além de implementar firewalls e protocolos de TI sofisticados, as empresas agora aumentam as habilidades de seus funcionários por meio de seminários, cursos e treinamentos. Afinal, 80% das violações de dados podem ser contornadas com a prática da higiene cibernética, conforme um estudo da Cyber Observer.

O que impulsiona a conscientização sobre o tema é o número crescente de pessoas que desconhecem a maioria dos métodos de ataque. Um relatório da Infosec indica que cerca de 97% da população mundial não consegue identificar um e-mail de phishing, enquanto 1 em cada 25 clica nesses e-mails. Para piorar, os golpistas agora recorrem a formas mais avançadas e de alta tecnologia de disseminação de phishing e malware.

Entretanto, a conscientização sobre a segurança digital pode ajudar a prevenir tais ataques. Empresas já implementam o uso combinado de métodos baseados na Web, sala de aula e plataformas gameficadas para treinamento e promoções de conscientização sobre o assunto. Além disso, criam políticas com foco em como os funcionários lidam e compartilham dados corporativos confidenciais – o que representa um avanço significativo.

Os ataques de phishing estão entre as ameaças mais difundidas. Como os cibercriminosos usam métodos mais sofisticados para criar ataques de comprometimento de e-mail comercial (BEC, na sigla em inglês), os e-mails de phishing e URLs maliciosos continuam causando estragos, exceto que agora são altamente localizados, mais personalizados e direcionados geograficamente.

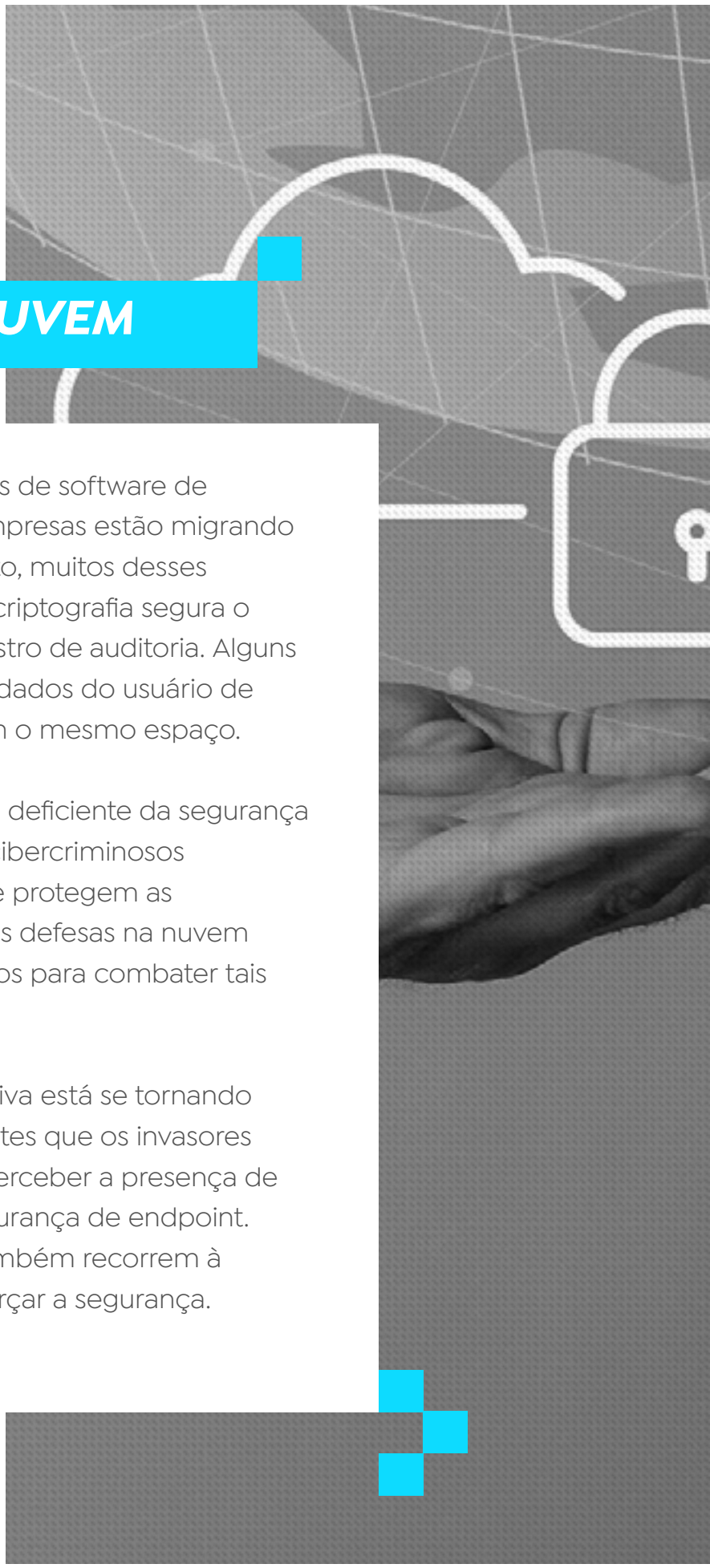
De acordo com o Relatório de investigações de violação de dados da Verizon, 32% das violações de dados no ano passado envolveram atividades de phishing. Assim, os especialistas acreditam que o phishing direcionado se tornará mais presente ainda nos próximos anos.

Também é importante observar que só em 2020 foram criados mais de 60.000 sites de phishing, e 1 em cada 8 funcionários compartilha informações indevidamente em algum destes sites – conforme pesquisa da Security Boulevard. Sendo assim, as empresas estão começando a adotar e investir em programas abrangentes de conscientização sobre segurança. Inclusive, estão implementando simuladores que podem explicar e reconhecer padrões de phishing e o modus-operandi desses ciberataques.

APRENDIZADO DE MÁQUINA

Na segurança cibernética, o papel do aprendizado de máquina (ML, na sigla em inglês) está crescendo e se tornando mais proativo. Com ele, a segurança cibernética fica relativamente mais simples, mais eficaz e, ao mesmo tempo, menos cara. A partir de um rico conjunto de dados, o ML desenvolve padrões e os analisa com algoritmos. Dessa forma, pode antecipar e responder a ataques ativos em tempo real.

Essa tecnologia depende fortemente de dados relevantes, que devem vir de diversas fontes e representar inúmeros cenários potenciais. Implementar o ML, portanto, permite que os sistemas de segurança analisem os padrões de ameaça e aprendam os comportamentos dos cibercriminosos. Isso ajuda a prevenir ataques semelhantes no futuro e também reduz o tempo necessário para que os especialistas em segurança cibernética executem tarefas de rotina.



SEGURANÇA NA NUVEM

Com a ajuda das melhores soluções de software de gerenciamento de nuvem, mais empresas estão migrando para o cloud computing. No entanto, muitos desses serviços ainda não oferecem uma criptografia segura o suficiente, com autenticação e registro de auditoria. Alguns também não conseguem isolar os dados do usuário de outros locatários que compartilham o mesmo espaço.

O problema é sério; a configuração deficiente da segurança em cloud pode fazer com que os cibercriminosos contornem as políticas internas que protegem as informações confidenciais. Assim, as defesas na nuvem estão ganhando conceitos preditivos para combater tais investidas.

Nesse contexto, a segurança preditiva está se tornando útil na identificação de ameaças antes que os invasores comecem sua ação. Afinal, pode perceber a presença de ataques que passam por outra segurança de endpoint. Ao mesmo tempo, as empresas também recorrem à autenticação multifatorial para reforçar a segurança.

VULNERABILIDADE DE IOT

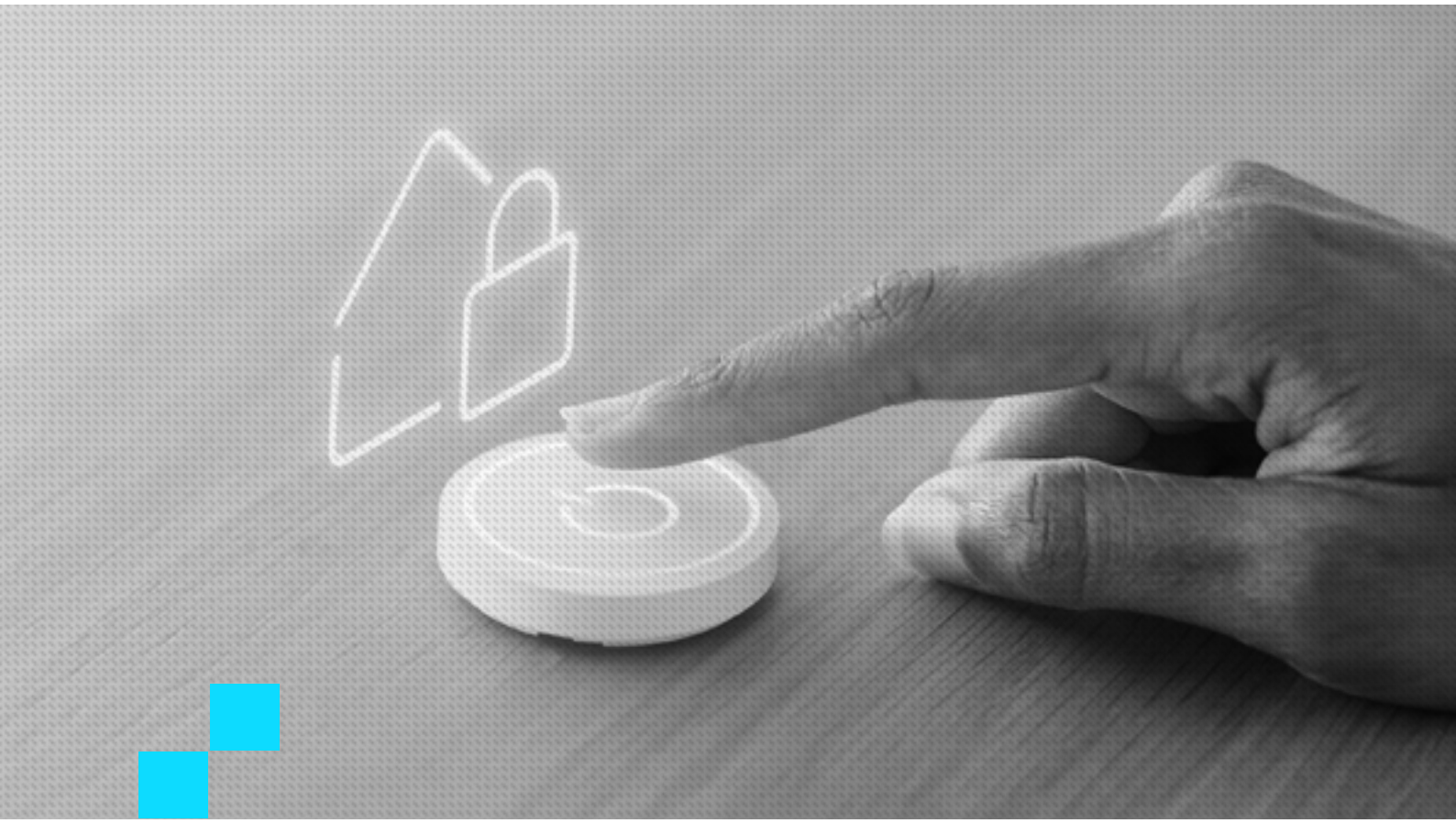
Equipamentos IoT estão aparecendo em partes da empresa que seriam impensáveis poucos anos atrás. Pode-se esperar que os dispositivos mais novos tenham conectividade com smartphones para fornecer serviços fora da área local e de redes Wi-Fi. Isso trará um modelo de assinatura que removerá as barreiras e a solução de problemas necessários para conectividade em redes domésticas ou de pequenas empresas.

A conectividade contínua será altamente atraente para a maioria dos usuários - especialmente em sistemas relacionados à segurança, como alarmes e câmeras.

Apesar da evolução nos dispositivos IoT, os problemas de segurança continuam afetando a maioria dos equipamentos que dominam o mercado hoje. Dispositivos de computação embutidos em produtos com essa tecnologia permitem o envio e recebimento de dados pela Internet. Isso representa ameaças de segurança significativas para os usuários, expondo-os a ataques cibernéticos.

Um relatório da Symantec revela que os roteadores infectados foram responsáveis por 75% de todos os ataques de IoT ocorridos em 2018, enquanto as câmeras conectadas foram responsáveis por 15% dos casos – indicando que o problema não é exatamente novo, mas segue vivo.

Apesar das ameaças contínuas, a análise de marketing do Boston Consulting Group indica que as empresas ainda estão investindo mais de US$ 267 bilhões em ferramentas de IoT. Isso vai ao encontro de um relatório mais recente, que mostrou que o setor de educação gastou 11,9% a mais em IoT em 2020 do que no ano anterior.



DISPOSITIVOS MÓVEIS COMO VETORES DE ATAQUE

A maioria dos principais softwares e plataformas de comércio eletrônico é acessível por meio de plataformas móveis, como tablets e smartphones. Os cibercriminosos veem isso como uma oportunidade de usar tais equipamentos como vetores de ataque.

É algo que cresce conforme as pessoas continuam a usar seus celulares para comunicações pessoais e comerciais, bem como para compras, internet banking, reservas de voos ou hotéis. De acordo com o artigo da RSA sobre o estado atual do crime cibernético, cerca de 70% das transações fraudulentas se originaram de plataformas móveis, com vetores populares de ataque móvel – incluindo malware, adulteração e perda de dados.

COMITÊS CIBERNÉTICOS

Com o aumento nas violações de segurança e na interrupção de negócios por conta de ransomwares, os conselhos das empresas estão se dedicando mais na proteção digital. Eles reconhecem isso como um grande risco para as empresas, e estão formando comitês dedicados a questões de segurança cibernética, geralmente liderados por um membro do conselho com experiência em segurança ou um consultor terceirizado.

Isso significa que os profissionais de segurança digital podem esperar um aumento nos recursos e também nas cobranças – algo natural quando há maior envolvimento da diretoria.

CONSOLIDAÇÃO DE FORNECEDORES

Uma coisa é fato: os profissionais de segurança possuem muitas ferramentas à sua disposição. A consultoria Gartner descobriu na Pesquisa de Eficácia CISO de 2020 que 78% dos diretores de segurança da informação (CISO, na sigla em inglês) têm 15 ou mais ferramentas em seu portfólio de fornecedores de segurança cibernética – sendo que 12% têm 45 ou mais. Isso resulta em operações de segurança complexas, bem como no aumento do número de funcionários ligados ao setor.

A maioria das empresas reconhece a consolidação de fornecedores como um caminho que leva a uma segurança mais eficiente, com 80% interessados – ou já executando – alguma estratégia nessa esfera. Nesse contexto, as desenvolvedoras de sistemas de segurança estão oferecendo produtos mais integrados. No entanto, a consolidação é um desafio que geralmente leva anos para ser implementada. Embora os custos mais baixos sejam frequentemente mencionados como benefícios dessa tendência, as operações mais simplificadas e riscos reduzidos se destacam na lista de vantagens.

SEGURANÇA E IDENTIDADE

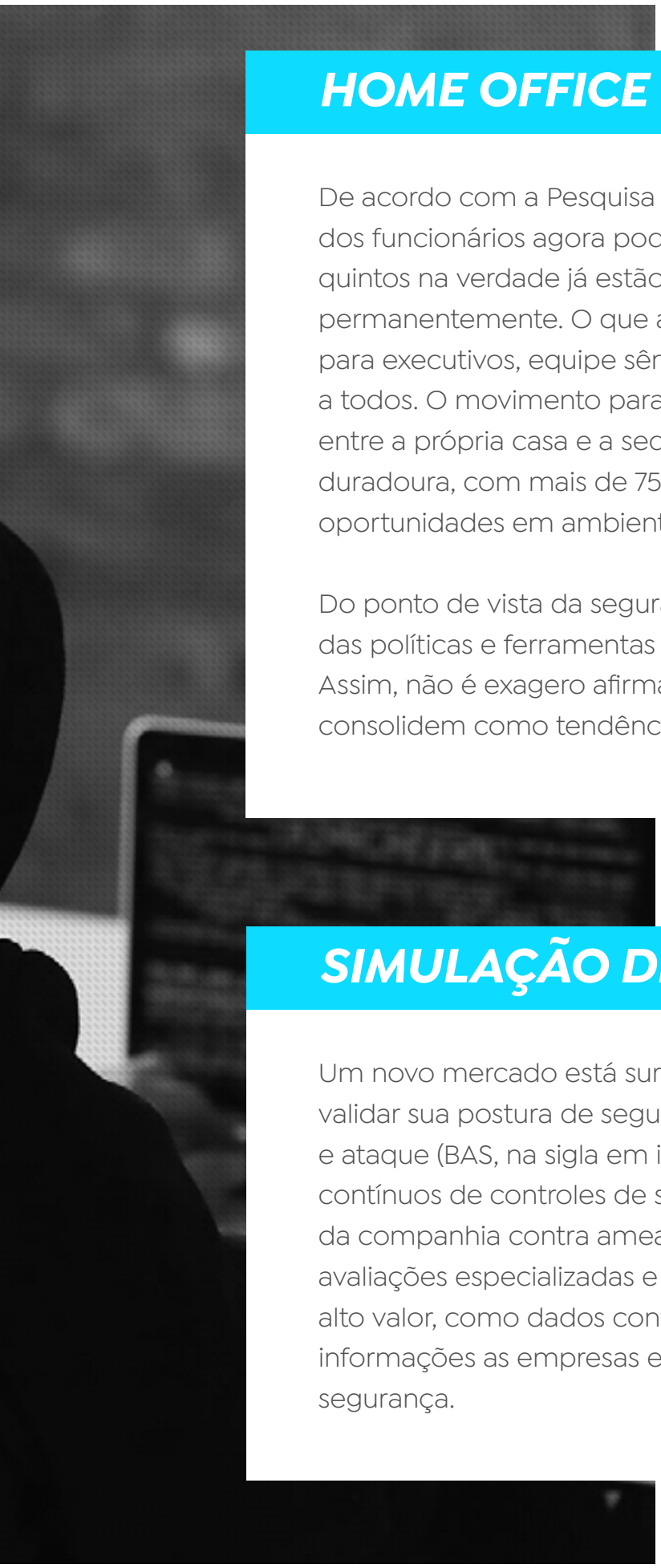
O home office e a migração para aplicativos em nuvem solidificaram a tendência da identidade como perímetro. A segurança que prioriza a identidade não é um conceito novo, mas assume uma nova velocidade à medida que os invasores começam a direcionar os recursos de gerenciamento de identidade e acesso para obter uma persistência silenciosa em uma eventual invasão.

Assim, credenciais mal utilizadas são agora a principal técnica usada em violações. Muitos cibercriminosos têm como alvo o Active Directory e a infraestrutura de identidade. A identidade é uma técnica-chave de movimento lateral em redes invadidas. O uso da autenticação multifator está crescendo, mas não resolve tudo sozinho. Por isso, a infraestrutura de identidade deve ser configurada, mantida e monitorada adequadamente o tempo todo.

IDENTIDADES DE MÁQUINA

Conforme a transformação digital avança, existe um forte crescimento no número de entidades não humanas que compõem os aplicativos modernos. Então, o gerenciamento de identidades de máquina se tornou uma parte vital das operações de segurança.

Todos os aplicativos modernos são compostos por serviços conectados por APIs. Cada um desses serviços precisa ser autenticado e monitorado, pois os invasores podem usar o acesso da API de seus fornecedores a dados críticos em seu benefício. As ferramentas e técnicas para gerenciamento de identidade de máquina em toda a empresa ainda estão surgindo. No entanto, uma estratégia corporativa para gerenciar identidades, certificados e segredos de máquinas permitirá que a empresa proteja melhor seu processo de transformação digital.



HOME OFFICE

De acordo com a Pesquisa de CIO da Gartner de 2021, 64% dos funcionários agora podem trabalhar em casa, e dois quintos na verdade já estão trabalhando em seus lares permanentemente. O que antes estava disponível apenas para executivos, equipe sênior e de vendas, agora é oferecido a todos. O movimento para o sistema híbrido (revezando entre a própria casa e a sede da empresa) é uma tendência duradoura, com mais de 75% dos trabalhadores esperando oportunidades em ambientes de trabalho híbridos no futuro.

Do ponto de vista da segurança, isso requer uma revisão total das políticas e ferramentas para mitigar melhor os riscos. Assim, não é exagero afirmar que soluções nesse sentido se consolidem como tendência para o próximo ano.

SIMULAÇÃO DE ATAQUE

Um novo mercado está surgindo para ajudar as empresas a validar sua postura de segurança. A simulação de violação e ataque (BAS, na sigla em inglês) oferece teste e validação contínuos de controles de segurança e põe à prova a postura da companhia contra ameaças externas. Também oferece avaliações especializadas e destaca os riscos para ativos de alto valor, como dados confidenciais. Em suma, o BAS oferece informações as empresas evoluírem suas estratégias de segurança.

AUMENTO DE PRIVACIDADE

As técnicas de computação que aumentam a privacidade e que protegem os dados enquanto eles estão sendo usados – ao contrário de quando estão em repouso – permitem o processamento, compartilhamento, transferências internacionais e análises de dados seguras, mesmo em ambientes não confiáveis.

Essa tecnologia está se transformando rapidamente de pesquisa acadêmica em projetos reais que oferecem valor real, permitindo novas formas de computação e compartilhamento com risco reduzido de violações de dados.

ALERTA PARA SEGMENTOS MAIS VISADOS PELOS CIBERCRIMINOSOS

Serviços financeiros

É fato que algumas empresas financeiras ainda lutam para acompanhar a migração para a nuvem e o número crescente de regulamentações. Além disso, os ataques de phishing continuam prevalecendo nesse setor, mas não apenas por e-mail. Surgem através de mídia social e outras plataformas de mensagens, que estão agora entre as tendências de segurança cibernética como ponto de atenção em serviços financeiros.

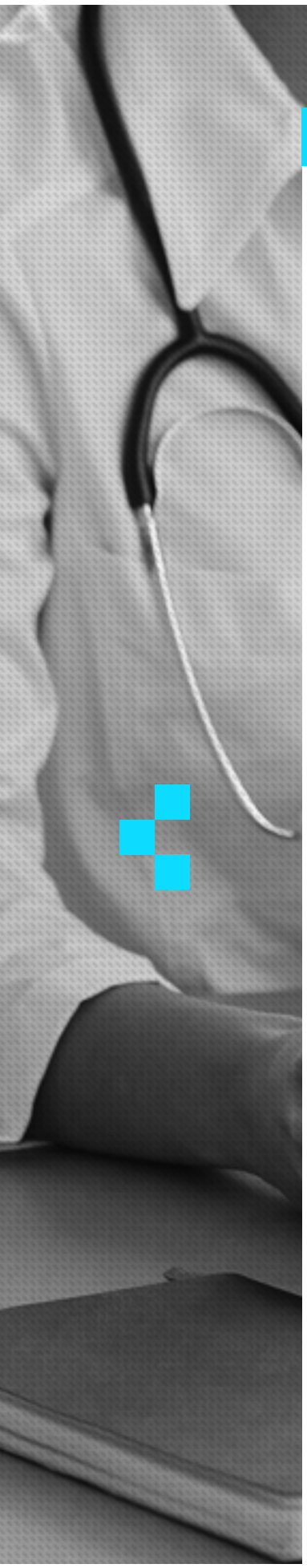
Outras ameaças mais comuns enfrentadas por seguradoras, bancos e gerentes de ativos incluem ataques de malware e violações de dados. Outro relatório do Boston Consulting Group revelou que o setor é cerca de 300 vezes mais suscetível a ataques virtuais do que as empresas de outras áreas. As invasões agora custam ao setor bancário US$ 18,3 milhões por empresa, segundo a Security Boulevard, o que torna esse segmento digno de cuidados extras no que se refere às tendências de proteção digital para o ano que vem.

Educação

A segurança cibernética segue entre as principais prioridades das faculdades e universidades, especialmente com o aumento do Ensino a Distância e do Home Office. Assim, os pontos de atenção envolvem principalmente a segurança dos dados de alunos e funcionários. Somente neste ano, três universidades privadas dos Estados Unidos foram vítimas de ataques cibernéticos que comprometeram dados de estudantes. Isso ligou o alerta dos responsáveis pela segurança digital no setor, que envolve também centros de pesquisa em universidades.

O problema, contudo, não é de hoje. O Relatório de Segurança Cibernética da Educação de 2018 do Security Scorecard apontou que, em termos de segurança cibernética, a educação vem em último lugar entre 17 setores nos EUA, um mercado que é referência para o Brasil. Além disso, o documento indica que o setor de ensino superior está tendo um desempenho insatisfatório na cadência de patches, segurança de rede e segurança de aplicativos.

Felizmente, as instituições agora estão adotando uma nova arquitetura de segurança que inclui segurança pós-perímetro na proteção de endpoint, acesso à nuvem e informações de identidade – o que leva a um prognóstico mais positivo.



Saúde

Deixar de combater as ameaças cibernéticas no setor de saúde é algo que expõe muitos pacientes e empresas a todos os tipos de questões de responsabilidade e segurança. Isso fez com que hospitais e clínicas investissem mais em defesas virtuais.

Há tempos as violações de dados estão entre as principais tendências de segurança cibernética na área de saúde. De 2015 a 2019, só nos Estados Unidos cerca de 157 milhões de registros foram expostos. Como resultado, as empresas passaram a prestar mais atenção aos seus requisitos de segurança digital. Isso impulsiona um crescimento considerável para o mercado de segurança cibernética no segmento.

O problema é que na pandemia alguns hospitais e clínicas relaxaram temporariamente suas regras de firewall para tornar mais fácil o home office. Também foi necessário expandir os serviços de “telemedicina” e criar instalações médicas temporárias que acabaram driblando alguns protocolos de segurança digital.

Nesse contexto, os ataques cibernéticos no setor de saúde estão longe do fim. As violações de dados representam uma ameaça constante, já que informações confidenciais sobre as empresas, funcionários e pacientes são cada vez mais valiosas nas mãos dos cibercriminosos – algo que tende a ganhar relevância em 2022.

Cadeia de suprimentos

Ataques do tipo alcançaram novos patamares em 2021, com violações direcionadas a softwares amplamente usados, incluindo Kaseya e SolarWinds. Infelizmente, invasões do tipo tendem a crescer.

Os ataques à cadeia de suprimentos ficarão mais sofisticados. As empresas precisam incluir a possibilidade de incidentes assim em seus planos de defesa, planejando uma resposta pública e privada.

CONCLUSÃO

Ninguém sabe exatamente o que o futuro reserva para a área da segurança digital. Muitos setores ainda estão descobrindo como fortalecer suas redes em meio ao caos e às incertezas da pandemia. Porém, essas tendências mais recentes nos dão uma ideia do que podemos esperar nos próximos anos.

Claramente, podemos notar que desenvolvedores e administradores de softwares de segurança de TI, vão estar ocupados por um bom tempo.

Ficou claro que ataques como phishing, ransomwares, malwares e violações de dados não terminarão tão cedo. Portanto, identificar áreas críticas de ataque e antecipar possíveis cenários de ataque pode ajudá-lo a evitar se tornar uma vítima de tais ataques.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog/

ostec

Segurança digital de resultados