Manter -se atualizado com o mais recente em segurança cibernética nunca foi tão fundamental quanto em 2024. Allianz, fornecedor de serviços financeiros, chamou os ataques cibernéticos deste ano para os negócios no Reino Unido e uma das principais preocupações para empresas de todos os tamanhos pela primeira vez. No entanto, muitos profissionais ainda estão no escuro sobre o que os eventos no primeiro trimestre nos dizem sobre a paisagem cibernética pelo resto do ano que pode ter consequências significativas.

A TechRepublic consultou especialistas do setor no Reino Unido para identificar as três tendências mais significativas em segurança cibernética – IA, zero dias e segurança da IoT – e fornecer orientações sobre como as empresas podem melhor manter seu forte.

O que você vai ler:

1. Ataques cibernéticos sofisticados com ai

Em janeiro de 2024, o Centro Nacional de Segurança Cibernética do Reino Unido alertou que a ameaça global de ransomware deveria aumentar devido à disponibilidade das tecnologias de IA, com ataques aumentando em volume e impacto. O risco para as empresas do Reino Unido é especialmente pronunciado, com um relatório recente da Microsoft descobrindo que 87% são “vulneráveis” ou “em alto risco” de ataques cibernéticos. O ministro da IA e a propriedade intelectual, Visconde Camrose, destacou especificamente a necessidade de as organizações do Reino Unido “intensificar seus planos de segurança cibernética”, pois é o terceiro país mais alvo do mundo quando se trata de ataques cibernéticos, depois dos EUA e Ucrânia.

James Babbage, diretor geral de ameaças da Agência Nacional de Crimes, disse no cargo do NCSC: “A IA atende barreiras mais baixas à entrada, aumentando o número de criminosos cibernéticos e aumentará sua capacidade, melhorando a escala, a velocidade e a eficácia da existência existente Métodos de ataque. ”

Os criminosos podem usar a tecnologia para encenar ataques de engenharia social mais convincentes e obter acesso inicial à rede. De acordo com o relatório global de previsão de segurança cibernética do Google Cloud, grandes modelos de idiomas e IA generativa “serão cada vez mais oferecidos em fóruns underground como serviço pago e usados para vários propósitos, como campanhas de phishing e desinformação de espalhamento”.

Veja: Principais previsões de IA para 2024 (Download de premium de TechRepublic gratuito)

Jake Moore, consultor global de segurança cibernética da empresa de segurança e antivírus da Internet, está investigando o software de clonagem em tempo real que usa a IA para trocar o rosto de um videochamador com a de outra pessoa. Ele disse ao TechRepublic por e -mail: “Essa tecnologia, juntamente com um impressionante software de clonagem de voz de IA, já está começando a fazer com que a autenticidade de uma videochamada questionável que possa ter um impacto devastador em empresas de todos os tamanhos”.

O Openai anunciou em 29 de março de 2024 que estava adotando uma “abordagem cautelosa e informada” quando se trata de liberar sua ferramenta de clonagem de voz ao público em geral “devido ao potencial de uso indevido de voz sintética”. O modelo chamado mecanismo de voz é capaz de replicar de forma convincente a voz de um usuário com apenas 15 segundos de áudio gravado.

“Os hackers maliciosos tendem a usar uma variedade de técnicas para manipular suas vítimas, mas novas tecnologias impressionantes sem limites ou regulamentos estão facilitando para os cibercriminosos influenciarem as pessoas para obter ganhos financeiros e adicionar mais uma ferramenta ao seu crescente kit de ferramentas”, disse Moore.

“Os funcionários precisam ser lembrados de que estamos mudando para uma época em que ver nem sempre acredita, e a verificação continua sendo a chave para a segurança. As políticas nunca devem ser cortadas em favor de instruções faladas e todos os funcionários precisam estar cientes do (software de clonagem em tempo real) que está prestes a explodir nos próximos 12 meses. ”

2. Explorações de dia zero mais bem-sucedidas

As estatísticas do governo descobriram que 32% das empresas do Reino Unido sofreram uma violação conhecida de dados ou ataques cibernéticos em 2023. Raj Samani, vice - presidente sênior Cientista da plataforma unificada de segurança cibernética Rapid7, acredita que os ataques corporativos permanecerão particularmente frequentes no Reino Unido ao longo deste ano, Mas acrescentou que os atores de ameaças também são mais sofisticados.

Ele disse ao TechRepublic em um email: “Uma das tendências mais emergentes de 2023 que estamos vendo continuar em 2024 é o grande número de zero dias explorados por grupos de ameaças que normalmente não previámos ter tais capacidades.

“O que isso significa para o setor de segurança cibernética do Reino Unido é a demanda por um trincho mais rápido da priorização de atualização de segurança. É imperativo que as organizações de todos os tamanhos implementem uma abordagem para melhorar a identificação de avisos críticos que afetam seu ambiente e que incorporem o contexto

nessas decisões.

“Por exemplo, se uma vulnerabilidade estiver sendo explorada na natureza e não há controles compensadores – e está sendo explorada por, por exemplo, grupos de ransomware – então a velocidade com que os patches são aplicados provavelmente precisarão ser priorizados”.

Veja: Top previsões de segurança cibernética para 2024 (download de premium do TechRepublic gratuito)

A “Pesquisa de violações de segurança cibernética 2023” do governo do Reino Unido encontrou declínios nas principais práticas de higiene cibernética de políticas de senha, firewalls de rede, direitos de administrador restritas e políticas para aplicar atualizações de segurança de software dentro de 14 dias. Embora os dados reflitam amplamente mudanças nas micro, pequenas e médias empresas, o frouxo aumenta significativamente o escopo dos alvos disponíveis para os criminosos cibernéticos e destaca a necessidade de melhoria em 2024.

“Os dados pessoais continuam sendo uma moeda extremamente valiosa”, disse Moore à TechRepublic. “Depois que os funcionários diminuíram a guarda (ataques) podem ser extremamente bem -sucedidos, é vital que os funcionários estejam cientes de (as) táticas que são usadas”.

Cobertura de segurança de leitura obrigatória

3. Foco renovado na segurança da IoT

Em 29 de abril de 2024, todos os fornecedores de dispositivos de IoT no Reino Unido precisarão cumprir a Lei de Segurança e Telecomunicações do Produto 2022, o que significa que, no mínimo:

1. Os dispositivos devem estar ativados por senha.
2. Os consumidores podem relatar claramente problemas de segurança.
3. A duração do suporte de segurança do dispositivo é divulgada.

Embora este seja um passo positivo, muitas organizações continuam a confiar fortemente em dispositivos herdados que podem não receber mais apoio de seu fornecedor.

Moore disse ao TechRepublic em um email: “Os dispositivos de IoT são frequentemente embalados com os recursos de segurança fracos-se houver-, para que os usuários (usuários) estejam no pé traseiro desde o início e geralmente não percebem as possíveis fraquezas. As atualizações de segurança também tendem a ser pouco frequentes, o que colocou mais riscos no proprietário. ”

As organizações que dependem de dispositivos herdados incluem aqueles que lidam com a infraestrutura nacional crítica no Reino Unido, como hospitais, serviços públicos e telecomunicações. As evidências de Thales apresentadas para um relatório do governo do Reino Unido sobre a ameaça de ransomware para a segurança nacional declararam: “Não é incomum dentro do setor da CNI encontrar sistemas de envelhecimento com longa vida operacional que não são rotineiramente atualizadas, monitoradas ou avaliadas”. Outras evidências do NCC Group disseram que “os sistemas de tecnologia operacional (OPRACIONAL) têm muito mais probabilidade de incluir componentes com 20 a 30 anos de idade e/ou usar software mais antigo que é menos seguro e não mais suportado”. Esses sistemas mais antigos colocam serviços essenciais em risco de interrupção.

Veja: os principais riscos de segurança do IIOT

De acordo com a empresa de segurança de TI Zscaler, 34 das 39 explorações de IoT mais usadas estão presentes em dispositivos há pelo menos três anos. Além disso, os analistas do Gartner previram que 75% das organizações abrigam sistemas não gerenciados ou herdados que executam tarefas de missão crítica até 2026 porque não foram incluídas em suas estratégias zero de confiança.

“Os proprietários da IoT devem entender os riscos ao colocar qualquer dispositivo conectado à Internet em seus negócios, mas forçar os dispositivos de IoT a serem mais seguros da fase de design é vital e podem consertar muitos vetores de ataque comuns”, disse Moore.

(Tagstotranslate) AI