Guia de Formação para cibersegurança

Conheça as ameaças que enfrenta a sua empresa

brother at your side | in[ctrl]

Em colaboração com KnowBe4 Human error. Conquered.

Em 2023 o custo médio de uma fuga de dados ascendeu a 4,05 milhões de euros[1], 15% mais que nos três anos anteriores.

Quando o trabalho remoto é a causa de uma violação ou roubo de dados, esse custo médio aumenta 157.506€[2].

54% das empresas afirma que os seus departamentos de TI não são suficientemente sofisticados para lidar com ciberataques avançados.[3]

Se um hacker tratasse hoje de atacar a sua empresa, teria sucesso? Se não pode confiar na cibersegurança da sua empresa então tem um grande problema. E não é o único.
Manter os sistemas de TI a salvo continua a ser um dos maiores desafios dos responsáveis da tomada de decisões na área tecnológica (ITDM). E o risco de que um destes ataques tenha sucesso nunca foi tão grande devido, por um lado, ao facto de as organizações estarem cada vez mais baseadas em sistemas digitais e, por outro, devido à sofisticação cada vez maior dos ciberciminosos.

Com base num estudo realizado pela Brother identificámos que, infelizmente, muitos departamentos de TI sentem que não estão preparados para fazer frente a isto. A falta de orçamento e de recursos/ferramentas apropriados são algumas das razões mais citadas quando se pergunta aos ITDM sobre as suas preocupações quanto aos ataques de cibersegurança e à sua capacidade para se defenderem deles com sucesso.

54% dos ITDM assegura que o investimento para manter a segurança dos sistemas tecnológicos está a aumentar.

No entanto, 44% acredita que manter a salvo estes sistemas de TI continua a ser o seu maior desafio e indica que talvez os investimentos não estejam a ser aplicados adequadamente.

Na Brother associámo-nos à KnowBe4 para analisar e avaliar a opinião e visão dos ITDM em relação aos riscos de segurança que enfretam as empresas nos dias de hoje e como implementar uma cultura de formação sobre esse tema, pode ajudar as empresas a manterem-se seguras e preparadas perante possíveis ameças.

Os humanos são a última linha de defesa quando falamos de cibersegurança e, embora qualquer problema a este respeito se considere competência do departamento de TI, a realidade é que todas as pessoas que trabalham numa empresa têm uma certa responsabilidade na hora de prevenir e evitar fugas de dados. Assegurar de que todos os colaboradores o entendem e oferecer a formação que necessitam para estarem atentos a possíveis ameaças de segurança, assim como ensinar o que fazer para as evitar, deveria fazer parte integral de qualquer estratégia de cibersegurança empresarial.

O erro humano é a causa de 95% dos ciberataques.[4]

Basil Fuchs
Chief Information Officer
Brother International Europe

"Os riscos da cibersegurança não param de crescer e isto é o resultado direto da sofisticação cada vez maior da engenharia social que utilizam os cibercriminosos para levar a cabo os ataques. As pessoas recebem inclusivamente mensagens sobre emails fraudulentos antes que estes cheguem à sua caixa de entrada, para os fazer parecer mais legítimos. E os cibercriminosos aproveitam-se do ritmo frenético dos profissionais que não têm tempo de analisar em detalhe todas as mensagens para procurar sinais de fraude".

[1]IBM [2]IBM [3]Sophos [4]IBM Cyber Security Intelligence Index Report

brother at your side | KnowBe4 Human error. Conquered.

As maiores ameaças que enfrentam as empresas

A Brother efetuou um exaustivo estudo no qual perguntou a ITDM de toda a Europa sobre as ameças de cibersegurança que enfrentam e que não se sentem preparados para gerir. Sem surpresa, costumam ser áreas onde o erro humano pode ser a chave para que o ataque tenha ou não sucesso.

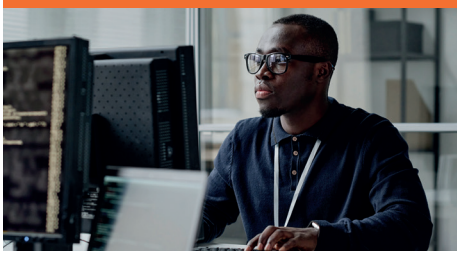
Neste guia analizaremos as três ameaças de cibersegurança que os ITDM afirmam que se sentem menos preparados para tratar, assim como as ferramentas e técnicas que as empresas podem adotar para reforçar as suas defesas e minimizar o risco de uma falha de segurança.

Estas ameaças são:

Ataques de phishing

Malware

Segurança da rede



Um dos maiores desafios que enfretam os ITDM é a necessidade de formação para reforçar essas áreas. No entanto, muitos não têm o tempo ou o orçamento necessários para isso. Assim, uma vez que as pessoas são a última linha de defesa em cada um destes casos, é fundamental que se ensine às equipas como identificar e responder aos riscos de forma rápida e precisa. Se não contam com os recursos necessários para o fazer internamente muitas empresas, como a Brother, decidem apoiar-se em parceiros para efetuar esta preparação e formação dos colaboradores.

Russell Johnson
Business Partner y Global Cyber Security Lead
Brother International Europe

"As empresas podem pensar que permitir que um terceiro intervenha nas suas práticas de cibersegurança vai contra a própria ideia de uma defesa cibernética eficaz. É por isso que muitas preferem realizar internamente a formação e o desenvolvimento desta parte fundamental para as suas atividades comerciais.

No entanto, a menos que as suas equipas estejam a par das técnicas mais recentes utilizadas pelos hackers, os funcionários não podem ser formados da melhor forma possível para manter as suas defesas cibernéticas, o que pode deixar os seus sistemas vulneráveis."

As pessoas têm o papel mais importante na hora de manter segura uma empresa

Também perguntámos no nosso estudo quais são os desafios tecnológicos que estão a aumentar ou a diminuir a sua importância e 50% dos ITDM assegura que manter a segurança dos sistemas de TI é um desafio cada vez maior. Os hackers estão constantemente a desenvolver novas ferramentas e técnicas, o que faz com que seja muito difícil para as organizações identificar e protegerem-se de forma eficaz perante os novos ataques. Entretanto, o crescimento da IoT (Internet of Things) continua, o que aumenta a área de ataque para os cibercriminosos.

Com tantos pontos de acesso a uma empresa e cada vez mais colaboradores a trabalhar em remoto desde múltiplos dispositivos e localizações, as pessoas que estão dentro de uma organização são com frequência a ligação mais débil a ter em conta em qualquer estratégia de cibersegurança. E, embora a equipa humana seja o maior ativo, também pode ser a maior debilidade, quer seja por falta de formação, por esquecimento , por não seguir as boas práticas de cibersegurança ou por erro.

Apenas 29% dos ITDM colocaria a formação dos utilizadores em matéria de segurança no primeiro lugar das suas prioridades.

Apenas 1 em cada 9 empresas britânicas ofereceu formação de cibersegurança aos funcionários não tecnológicos em 2022.

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

"A tecnologia e a formação estão interligadas quando se trata de educação na segurança, uma vez que a primeira é aproveitada para a segunda: a tecnologia facilita módulos interativos, exercícios de simulação de *phishing* e acesso a recursos online, todo isso para garantir que os colaboradores captam os principios da cibersegurança de forma eficiente. Por seu lado, a formação complementa a tecnologia incutindo o pensamento crítico e as as melhores práticas, e dando aos colaboradores a capacidade para reconhecer e responder às ameaças. Juntas criam um ambiente de aprendizagem dinâmico onde os trabalhadores não só entendem os riscos de cibersegurança, como também desenvolvem as habilidades necessárias para os mitigar. É necessário realizar atualizações regulares e implementar mecanismos de feedback para estarem alinhados com um panorama de ameaças em evolução, criando uma cultura de vigilância e resiliência dentro da organização."

Os hackers não têm escrúpulos na hora de atacar empresas de qualquer tamanho. No entanto, tendem a ser os negócios pequenos e médios, que não têm realizar investimentos importantes em cibersegurança, os que podem estar em maior risco. E, com a prática cada vez mais habitual do teletrabalho, é especialmente importante para as empresas de qualquer tamanho, garantir que os seus colaboradores seguem as melhores práticas nesta área.

Criando uma cultura de cibersegurança dentro da organização

A formação contínua em cibersegurança deveria fazer parte do desenvolvimento de qualquer colaborador. No entanto, não é tão comum como deveria. Uma formação em cibersegurança eficiente é muito mais que oferecer aos trabalhadores programas de consciencialização de forma intermitente. As organizações que estão verdadeiramente preparadas para os ataques e que têm a melhor defesa face a eles têm a cibersegurança incluída na sua cultura e colaboradores que, sem darem conta, reforçam as suas defesas diariamente.

Russell Johnson
Business Partner y Global Cyber Security Lead
Brother International Europe

"A Brother está muito comprometida com a criação de uma cultura de cibersegurança em toda a empresa. Isto porque entendemos que a cibersegurança não é um exercício de 'marcar casas'. É uma responsabilidade coletiva e constante. A nossa cibersegurança é tão forte como são as nossas pessoas e portanto, como organização, a melhor forma de nos protegermos é investir nelas e dar-lhes o conhecimento e as habilidades que necessitam para identificar e responder as ciberameaças em qualquer momento ou lugar em que ocorram."

60% dos ITDM afirma que o departamento de TI é responsável pela formação em ciberseguranĕa de toda a empresa.

Russell Johnson
Business Partner y Global Cyber Security Lead
Brother International Europe

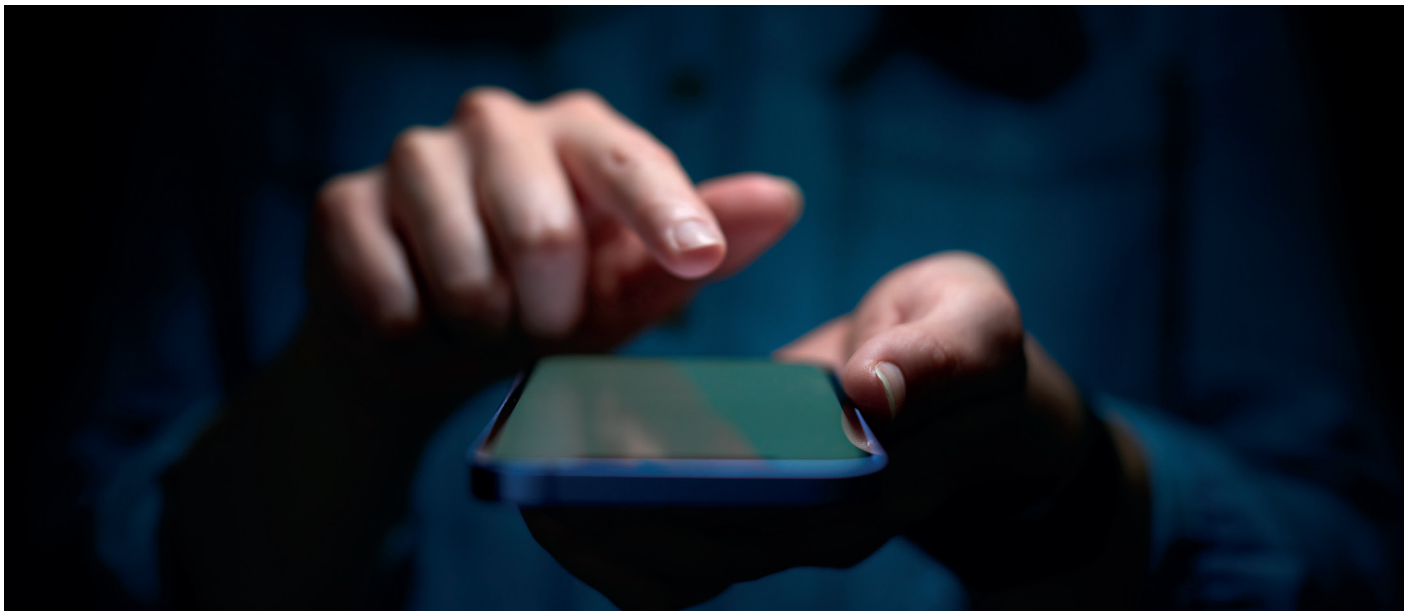
"Nos últimos anos aumentámos drasticamente o nosso conhecimento sobre cibersegurança dentro da Brother, mediante testes de conhecimento em cibersegurança e formação corretiva automática, especificamente dirigida e baseada nas debilidades identificadas. Complementamos isto com envios a cada duas semanas, mais ou menos, com notícias e tendências da atualidade sobre cibersegurança e com encontros trimestrais interativos com oradores convidados que realmente sensibiliza as nossas equipas sobre os últimos desenvolvimentos a que têm que estar atentos."

Conselhos chave para involver os colaboradores em cibersegurança

O estudo sugere que são os departamentos de TI os responsáveis por criar uma cultura de cibersegurança dentro de qualquer organização, o que pode ser difícil para aqueles com conhecimentos e recursos limitados. Dito isto, em qualquer organização deveriam ser dados passos rumo à proteção cibernética.

Por exemplo:

- Criar conteúdos e materiais de formação que todos os trabalhadores da empresa entendam, a todos os níveis;
- Assegurarmo-nos de que o conteúdo que usamos para oferecer a formação é claro, relevante e está suportado por exemplos do mundo real que o mostram em ação;
- Ofereçê-la num formato que possa ser utilizado por qualquer um dos seus públicos e que torne a informação memorável;
- Utilizar diferentes técnicas para que a educação em cibersegurança faça parte da cultura empresarial, como *newsletters,* vídeos, posters e, inclusivamente, eventos;
- Para organizações internacionais, garantir que o conteúdo não só se traduz de forma apropriada, mas também adaptada às diferentes regiões para ter um maior impacto;
- Promover uma boa relação entre o departamento de tecnologia e o resto dos colaboradores, dando feedback positivo e reconhecimento aqueles que reportem comportamentos ou emails suspeitos, para que saibam que as contribuições são apreciadas;
- Incentivar os diretores a partilhar as suas experiências e liderar com o exemplo.



Ataques de *phishing*

Phishing é quando um cibercriminoso se faz passar por uma pessoa ou empresa legítima - normalmente por email, redes sociais ou telefone - para tentar obter informação sensível como palavras-passe ou números de cartões de crédito. Também se usa como uma ferramenta para distribuir *malware.* O *phishing* continua a ser um dos métodos mais populares em ciberataques.

74% das fugas de dados inclui o fator humano.[5]

Tendo em conta que as organizações se baseaim em grande medida em canais de comunicação digitais, estes convertem-se numa perfeita via de entrada para os cibercriminosos. No entanto, talvez a única forma de evitar um *ataque de phishing* é que os colaboradores sejam capazes de o reconhecer e evitar.

Infelizmente, as fraudes com *phishing* implicam normalmente fazer-se passar por marcas bem conhecidas como Microsoft, Amazon ou Google para enganar os utilizadores. De facto, só em 2022 mais de 30 milhões de mensagens fraudulentas de *phishing* mencionavem produtos da Microsoft.[6]

28% dos ITDM de pequenas empresas afirma que os ataques de phishing são as falhas de cibersegurança que se sentem mais mal preparados para gerir.

96% das empresas britânicas são vítimas de ataques de phishing na Europa, seguidas por 94% das empresas em Espanha, 85% em França e 79% em Itália.[7]

[5]Relatório Data Breach Investigation 2023 de Verizon [6]Forbes, 2023 [7]IT Governance

brother at your side | KnowBe4 Human error. Conquered.

Como podem os ITDM proteger-se contra ataques de phishing?

Sabendo que os ataques de *phishing* se aproveitam das debilidades humanas, a única forma real de tentar proteger a empresa face a eles é assegurar-se de que todos os colaboradores estão bem formados para os identificar e sabem o que fazer se suspeitam de algum. E, considerando que os métodos de *phishing* evoluem constantemente, esta formação não deveria ser um evento único, mas sim como uma atualização regular que se dá a todos os empregados, seja qual for o posto dentro da organização.

Como camada de proteção adicional, os ITDM também podem implementar soluções de software de proteção face ao *phishing.* Tratam-se de ferramentas que analizam distintas variáveis das mensagens e alertam ou bloqueiam o conteúdo suspeito, evitando que chegue à caixa de entrada ou ao navegador.

As bandeiras vermelhas do *phishing*

O sucesso de um ataque de *phishing* baseia-se na necessidade de enganar os colaboradores para que cliquem e/ou partilhem algo que não deveriam. A única maneira de evitar que o façam é mediante formação contínua e recordatórios acerca de quais são as 'red flags' que poderiam indicar que uma mensagem é uma tentativa de fraude.

As bandeiras vermelhas que deveriam procurar incluem:

- Uma mensagem que vem de um domínio que não é o mesmo que o da empresa a que supostamente pertence;
- URLs que não coincidem com um endereço web;
- Erros gramaticais ou ortográficos;
- Fontes de letra invulgares, especialmente se a fonte parece mudar a meio de uma palavra;
- A tentativa de criar um sentido de urgência: "este link expira em 48 horas" ou "valide rapidamente a sua identidade".
- Saudações invulgares num email profissional como "Olá querido".

Qual é a capacidade das suas equipas para identificar um e-mail ou uma mensagem fraudulentos? Costumava ser bastante simples fazê-lo graças aos erros ortográficos e gramaticais óbvios, mas graças à IA generativa, que está a ajudar os infratores a evitá-los, detetar mensagens de *phishing* é agora mais difícil que nunca. Uma forma de saber o nível de preparação dos seus equipamentos é estabelecer a sua percentagem Phish-prone™.

A realização regular de testes de *phishing* deveria portanto ser parte integral do plano de cibersegurança de qualquer organização.

Russell Johnson
Business Partner y Global
Cyber Security Lead
Brother International Europe

"Implementámos uma série de passos para minimizar o risco de sofrer um ataque de *phishing.* Algumas das simulações que colocámos em marcha como parte da nossa estratégia de cibersegurança incluem:

- **Emails relacionados com recursos humanos, utilizando argumentos como doenças, férias anuais ou assinatura de novas políticas;**
- **Emails relacionados com os diretores, por exemplo, pedindo aos colaboradores que abram/assinem/leiam rapidamente documentos;**
- **Emails relacionados com os sistemas, como links para assinar um documento no Google ou aceder ao SharePoint."**

Percentagem Phish-prone™: O que é e porque é importante

A sua percentagem de propensão ao *phishing (phish-prone)* é o rácio de colaboradores propensos a clicar num link ou interagir com uma mensagem fraudulenta de forma não segura. Por exemplo, introduzindo dados numa página web falsa, abrindo um anexo ou respondendo à mensagem.

Esta percentagem de propensão ao *phishing* calcula-se dividindo o número de colaboradores que foi vítima num teste de *phishing* pelo número de colaboradores que foram testados. Depois, o resultado multiplica-se por 100 para conseguir a percentagem. Por exemplo, se uma organização tem 100 colaboradores e 20 deles clicaram no falso email fraudulento durante a simulação, a percentagem seria de 20%.

"Não entre em pânico se o seu indicador de propensão ao *phishing* é mais alto do que esperava, é bastante comum se não efetuou nenhum teste antes.
Na Brother fomos capazes de reduzir consideravelmente o nosso, num espaço relativamente curto de tempo, utilizando uma série de ferramentas de formação e testes de simulação de *phishing.*
De facto, agora estamos abaixo da média do nosso setor, que é de 6%, o que prova o impacto que pode ter um modelo de teste constante e formação regular."

Testes de *phishing* e formação contínua

Os testes de *phishing* são uma das formas mais efetivas de descobrir o nível de preparação das equipas para gerir um ataque de *phishing*, no caso de a organização sofrer um, assim como reduzir a percentagem de propensão ao *phishing*.[8] A premissa é simples: as empresas que querem avaliar a sua equipa colocarão em marcha envios de *phishing* simulados (internamente ou através de um parceiro especializado) que tratam de enganar os colaboradores para que difundam informação sensível, mas sem nenhum risco real. Há múltiplas formas através das quais se pode tentar obter esta informação e, no final dos testes, calcula-se a percentagem de propensão ao *phishing* e compara-se com outros do mesmo setor (como dado de referência).

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

"O relatório de 2023 sobre Phishing por Setores da KnowBe4 revela que 33,2% dos utilizadores não formados cairá num teste de *phishing.* No entanto, implementando formação em segurança e compromentendo-se em desenvolver uma cultura em cibersegurança, as empresas demonstraram que é possível reduzi-lo abaixo da média do setor 5,9%."

Russell Johnson
Business Partner y Global Cyber Security Lead
Brother International Europe

"Na Brother reduzimos, consideravelmente, a nossa percentagem de propensão ao *phishing* nos últimos anos. Como? Começámos com uma bateria de testes de *phishing* em março de 2022, que mostrou que a nossa percentagem de propensão ao *phishing* (PPP) era de 11,5%. Seguidamente, implementámos um plano de formação sólido e fizemos testes sobre as capacidades de reconhecimento de possíveis fraudes aos colaboradores para identificar os principais pontos débeis. Com tudo isso fomos capazes de organizar uma formação corretiva especialmente orientada para cobrir as carências identificadas. Enviámos mais de 30.000 emails de *phishing,* 17.000 no último ano. Atualmente o nosso PPP é de apenas 5,2% e o nosso objetivo é estar abaixo de 2%".

A obtenção do dado de referência quanto ao *phishing* desenvolve-se em três fases:

Fase um: envia-se a todos os utilizadores um email fraudulento simulado antes de receberem qualquer formação. O número de pessoas que cai na armadilha vai-nos dar a percentagem base. Em média, 33,2% dos trabalhadores será vítima de um email fraudulento.

Fase dois: 90 dias depois desse primeiro email fraudulento simulado, os utilizadores já tiveram que completar a formação e já receberam testes de *phishing.*

Fase três: repete-se o teste doze meses depois.

O que os dados mostram, com base em 32,1 milhões de emails fraudulentos para 12,5 milhões de utilizadores, é que os resultados do teste de phishing após noventa dias de formação, baixam de 33,2% para 18,5%. Este valor desce ainda mais, para 5,4%, após doze meses.

As percentagens variam conforme o setor, a localização e o tamanho da organização.

91% das tentativas de fuga de dados que têm sucesso começam com um ataque de *spear-phishing.*[8]

O que é o *spear-phishing*

Trata-se de um ataque de *phishing* dirigido a indivíduos ou organizações específicas, normalmente através de emails maliciosos. O objetivo do *spear-phishing* é roubar informação sensível como credenciais de acesso ou infetar o dispositivo com *malware.*

[8]KnowBe4

Malware

Um dos maiores desafios que os ITDM acreditam que enfretam é a ameaça de que um tipo de software muito específico chamado *malware* entre na infraestrutura de TI.

34% dos ITDM de pequenas e médias empresas afirma que o *malware/ransomware* é o problema de cibersegurança para o qual se sentem menos preparados para enfrentar.[9]

O que é o *malware*

O *malware* é um tipo de software desenhado especificamente para interromper, danificar ou aceder sem autorização a um sistema informático. Como sabemos, os ataques de *phishing* usam-se frequentemente como uma maneira de introduzir *malware* nos nossos sistemas – fazendo-nos clicar num link ou descarregar anexos numa mensagem fraudulenta sem darmos conta de que são maliciosos.

Outras formas em que o *malware* pode entrar no seu dispositivo podem ser:

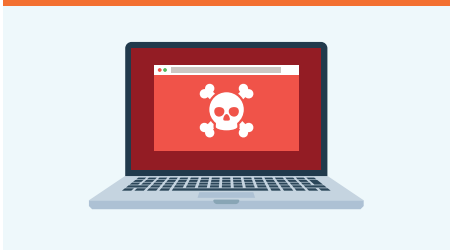
- Descargas automáticas desde webs comprometidas;
- Instalando software infetado no seu dispositivo;
- Suportes externos: USB e discos duros externos;
- Software desatualizado que tem vulnerabilidades de segurança.

Só em dezembro de 2023 houve na Europa mais de 100.884.532 registos de tentativas de fraude.[10]

[9]2023 Brother X Savanta ITDM priority survey [10]IT Governance

Os tipos de *malware* mais perigosos: um resumo

Troianos



Um troiano é um vírus que pode danificar os seus arquivos, modificar os seus dados, monitorizar a sua atividade, roubar informação sensível do seu dispositivo, redirigir tráfico de internet ou inclusivamente estabelecer pontos de acesso da porta traseira aos seus sistemas. E tudo sem que dê conta.

Ransomware

O *ransomware* é um tipo de software malicioso que está desenhado para bloquear o acesso ao seu dispositivo e aos dados armazenados nele até pagar um resgate ao atacante. Para isso, normalmente encriptam os seus arquivos de forma que não os possa ver nem atualizar.

Worms

Os worms são um tipo de vírus troiano. A sua função principal é autoreplicar-se e infetar outros dispositivos, enquanto se mantêm ativos em qualquer sistema que tenham infetado previamente.

Como podem proteger-se os ITDM face a ataques de *ransomware*

Em janeiro de 2023 o Royal Mail foi atacado por um dos ransomware mais perigosos do mundo: LockBit. O resgate solicitado foi de 80 milhões de dólares.[11]

Como sabemos, muitos ataques de *ransomware* são distribuídos através de campanhas de *phishing* nas quais os utilizadores clicam em links ilegítimos que descarregam software não seguro para os seus dispositivos. Portanto, uma das formas mais efetivas de proteger a organização face a este tipo de ameaças é assegurar que os colaboradores sabem como identificar e evitar essas campanhas. Associar-se a um parceiro fiável pode indicar exatamente o nível de eficiência das equipas para o fazer.

Outros passos que pode dar para evitar ataques de *ransomware* são:

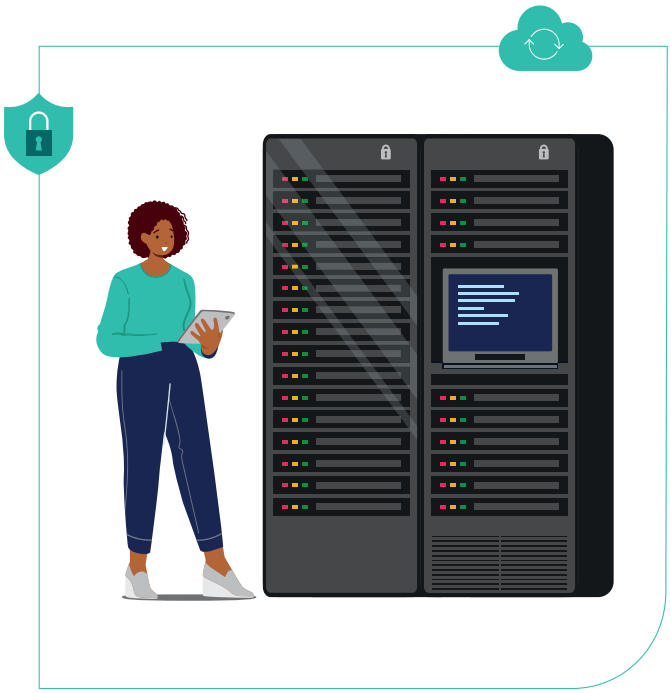
- Manter o software atualizado;
- Implementar a autentificação de dois fatores, especialmente para trabalhadores em remoto;
- Pedir aos utilizadores que mudem regularmente as suas palavras-passe;
- Utilizar hardware e software de segurança incluindo *firewalls,* aplicações de digitalização de emails e software antivírus;
- Realizar back-ups de forma regular e guardar toda a informação num ambiente de rede separado.

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

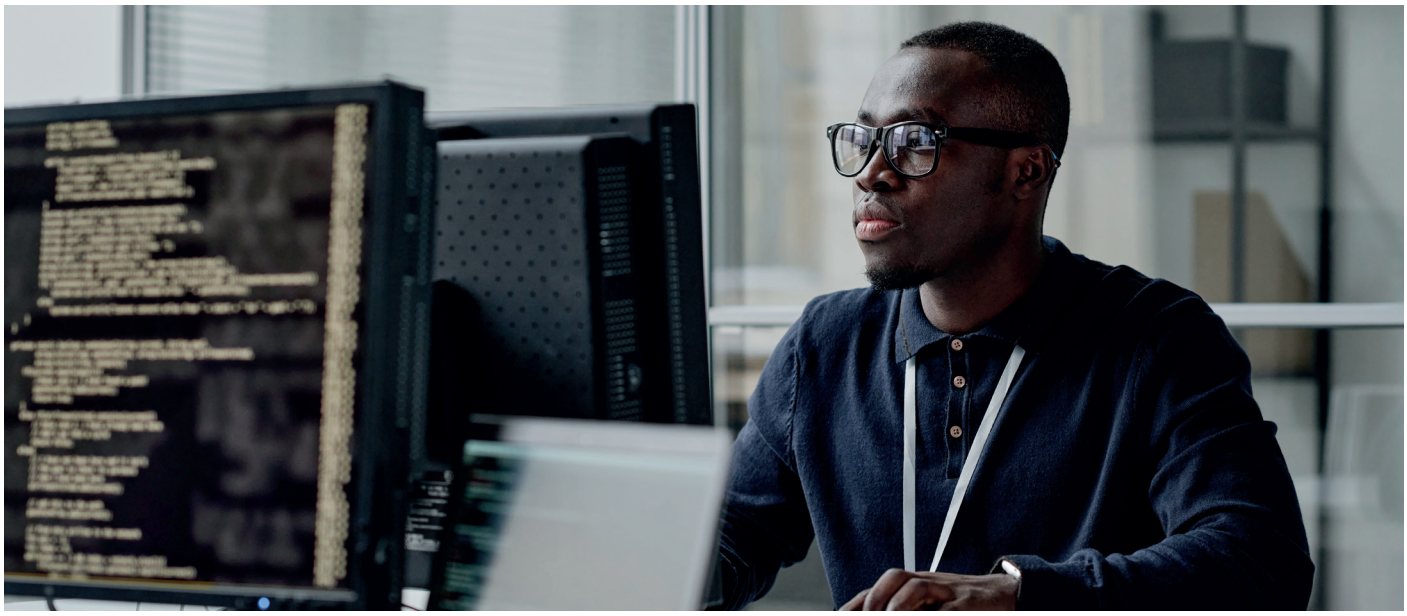
"Para combater o *ransomware* as organizações podem utilizar ferramentas como RanSim que dá uma visão 360º do seu nível de preparação perante um ataque. RanSim simula 24 cenários diferentes de infeção por *ransomware* e um cenário de prospeção de criptomoedas para determinar se um posto de trabalho é vulnerável"

Outra opção é implementar SOAR – segurança, organização, automatização e resposta -, um sistema especificamente desenhado para a gestão das ameaças de *phishing* e que pode reduzir o tempo de resposta e mitigar estas ameaças antes que cheguem às caixas de entrada da equipa.[12] Esta atitude proativa face ao *phishing* conta com capacidades como:

- Respostas automatizadas de email que permitem que os departamentos de TI comuniquem rapidamente com os empregados reduzindo o tempo de interrupção das operações;
- Identificação de padrões que permite que as equipas de resposta de incidentes reconheçam rapidamente ataques de grande difusão;
- Pegue em ataques do mundo real e transforme-os em modelos de simulação para os usar em programas de formação que melhorem as capacidades e experiência dos colaboradores.



[11]bbc.co.uk [12]KnowBe4



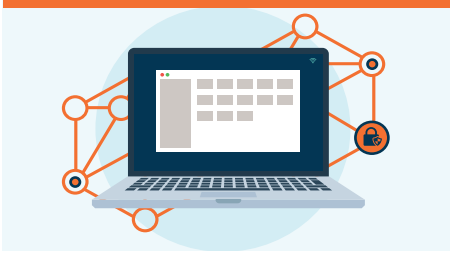
Segurança de rede

Algo que muitas vezes passa ao lado das empresas é a segurança da rede. Sabemos que isto é um problema que pode ter enormes implicações. No entanto, segundo o nosso relatório, está claro que é uma prioridade que muitas vezes não se tem em conta. A segurança da rede refere-se aos processos e ao software utilizados para proteger os computadores, impressoras, rede e dados. Normalmente divide-se em três áreas:

Física

Controlos de segurança utilizados para evitar acessos não autorizados às redes físicas como impressoras, routers e discos duros *(endpoints).*

Técnica



Segurança que protege os dados que entram, que saiem e os que estão armazenados na rede.

Administrativa

Controlos de segurança para o comportamento dos utilizadores, como quem tem acesso e que passos de autentificação usam.

A parte menos segura de qualquer rede são os dispositivos e, por isso, de novo entram em jogo os utilizadores. O trabalho híbrido criou novos desafios para as organizações e para a segurança da rede. Há uma maior superície de ataque com cada vez mais pontos de acesso para os cibercriminosos e, além disso, os trabalhadores remotos podem, inclusivamente, aceder aos servidores da empresa a partir de redes públicas, as quais oferecem uma proteção muito menor. Por tudo isso, também é mais difícil para as equipas de TI identificar e responder a eventuais ataques.

Basil Fuchs
Chief Information Officer
Brother International Europe

"No flexível e digital panorama de trabalho atual, garantir a segurança das redes é crucial para proteger os dados sensíveis. O modelo Zero-Trust, que assume que não há confiança inerente, garante que todos os utilizadores e dispositivos são verificados antes de lhes conceder acesso. Limitando o acesso a 'apenas o que é necessário', esta abordagem reduz o risco de qualquer movimento não autorizado".

O modelo de segurança Zero-Trust é muito eficiente, já que garante que os utilizadores só têm acesso e permissões para o que necessitam para realizar o seu trabalho. É uma abordagem muito diferente à da VPN standard, que dá acesso aos utilizadores a toda a rede. O benefício de uma abordagem de confiança zero é que, se qualquer utilizador estiver comprometido, os hackers só serão capazes de aceder aos dados a que este tiver acesso e não à rede inteira.

Algumas boas práticas para melhorar a segurança da rede:

1. Utilizar certificados SSL;
2. Pedir aos trabalhadores remotos para encriptar a sua wifi doméstica com encriptação WPA2;
3. Mudar o nome do router e a palavra-passe para disfarçar a sua identidade;
4. Desabilitar os WPS nos routers;
5. Enviar recordatórios a todos os utilizadores para que realizem *backups* dos seus dispositivos, incluindo impressoras, scanners, etc., regularmente e instalar atualizações quando estão disponíveis.

Como abordar a segurança da rede

A segurança da rede inclui muitos elementos distintos, todos essenciais. Isto é especialmente assim na era do trabalho híbrido e remoto, onde não só não é possível que os ITDM visitem e verifiquem todas as instalações domésticas, como nem sequer podem ver fisicamente as pessoas com regularidade. Tendo tudo isso em conta, estes seriam os nossos principais conselhos para garantir que todas as frentes estão cobertas.

Utilize certificados SSL

Se faz algum tipo de venda através da sua rede é fundamental um certificado SSL (Secure Sockets Layer) e utilizar HTTP. Um certificado SSL garante que nenhum dado partilhado entre os seus servidores e os seus clientes pode ser roubado por um terceiro, já que o certificado confirma a identidade do servidor e estabelece um canal de comunicação encriptado para permitir as compras.

Mantenha atualizado o *firmware* do router

Isto é especialmente importante para trabalhadores remotos, uma vez que o firmware do router vem pré-instalado no seus dispositivos. Este *firmware* deve ser atualizado pelo menos uma vez por ano para oferecer a melhor defesa possível perante ciberataques.

Utilize WPA2

WPA2, o WiFi Protected Access2, é um dos algoritmos de segurança mais fortes e complexos para salvaguardar uma rede WiFi.

Implemente uma VPN

As redes privadas virtuais ou VPN são essenciais para trabalhadores remotos, uma vez que reduzem os riscos de que a informação seja intercetada enquanto viaja entre redes. As VPN ajudarão a evitar que estes trabalhadores utilizem redes públicas vulneráveis de forma acidental.

Instale os *firewalls*

Pode parecer óbvio, mas uma firewall forte é ainda uma das armas de cibersegurança mais efetivas. Assegure-se de que tem tanto uma firewall interna como uma externa e contemple a opção de utilizar *firewalls* baseadas em camadas de hardware e software. Assegure-se também de que são atualizadas regularmente para uma maior proteção.

Desative a opção de partilhar ficheiros

Embora a colaboração seja fundamental para os trabalhadores remotos, o facto de partilhar ficheiros apresenta uma oportunidade real para os hackers de aceder à informação sensível ou causar danos nos seus sistemas. Implementar sistemas baseados na nuvem ou protegidos com palavras-passe permitirá a colaboração sem deixar a rede vulnerável.

Assegure os dispositivos

Especialmente as impressoras. As impressoras e outros equipamentos, como os scanners e discos duros portáteis, são muitas vezes esquecidos no que diz respeito à segurança da rede. Assegure-se de que o seu software está atualizado e considere implementar Secure Print+, uma funcionalidade que permite aos utilizadores atrasar a impressão real até que estejam fisicamente diante da impressora.

Segurança da impressão

Uma área de risco dos dispositivos de rede que muitas vezes é esquecida é a segurança das impressoras. As impressoras costumam considerar-se dispositivos bastante seguros, mas a verdade é que podem ser utilizadas pelos hackers como uma porta traseira para aceder à rede. E isto acontece com mais frequência do que se pensa.

Mais de um em cada dez incidentes de segurança que afeta uma empresa está relacionado com uma impressora.[13]

Isto porque a maioria das atuais impressoras estão conectadas à internet e esta conexão à rede tem dois sentidos: do dispositivo à impressora, mas também da impressora de volta ao dispositivo. E, embora os utilizadores não pensem duas vezes ao imprimir informação sensível, esta conexão de dois sentidos pode ser explorada por hackers experientes se a impressora não contar com sistemas de proteção tão robustos como o computador.

Segudo o relatório da Brother, 95% das empresas preocupam-se em garantir a segurança da rede para os seus trabalhadores híbridos.

Segurança by Brother é a nossa abordagem baseada em soluções para a segurança dos dispositivos que faz com que a impressão corporativa seja segura. Introduzimos a segurança de três níveis: rede, dispositivo e documento, para garantir que a informação só é vista por aqueles a quem se destina.

[13]Quocirca.

E para terminar...

Verificámos que uma abordagem “devo ter” e “seria bom ter” quanto à redução de riscos é a melhor maneira de garantir que os orçamentos dos ITDM são gastos de forma eficiente. Assim, podemos dividir os elementos relativos à cibersegurança em:

Imprescindíveis: São essenciais para uma proteção real, como uma firewall configurada, software antivírus, VPN, formação básica em cibersegurança e gestores de palavras-passe.

Valor acrescentado: Poderiam ser benéficos, mas não são fundamentais num nível de cibersegurança básico, como a autenticação multifatorial e sessões de formação regulares.

Depois de identificar os maiores riscos das organizações, este método permite determinar que medidas de segurança são cruciais para manter segura a empresa e quais poderiam ser muito benéficas se houvesse orçamento disponível. Também é uma boa forma para os IITDM conseguirem orçamento adicional para ter uma defesa mais forte.

No fim de contas, a cibersegurança não é só mais uma da longa lista das formações de rotina para as empresas. Para manter os sistemas e dados seguros, a cibersegurança necessita converter-se numa forma de vida entre as equipas e que assim se detetem riscos cibernéticos de forma tão natural como o fazem com os riscos de acidente na estrada quando estamos a conduzir.

Conheça as ameaças

Contacte um especialista em segurança da Brother

brother at your side | in[ctrl]

Em colaboração com KnowBe4 Human error. Conquered.