apfs

TEMA DO MÊS
Novembro 2025

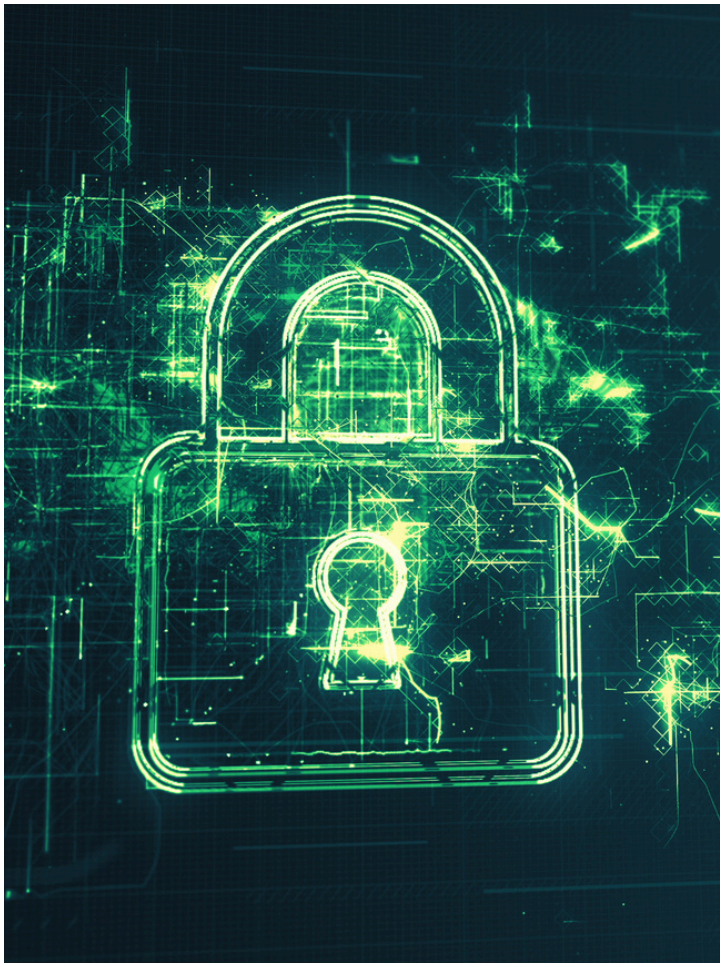
Segurança cibernética - tome medidas agora

Os grupos de ransomware têm como alvo apenas grandes corporações, certo? Bem, se acredita nisso, não só está a enganar-se a si mesmo, como também pode estar a deixar a sua empresa perigosamente exposta, escreve Hartley Milner.

A partir de um único cavalo e carroça em 1865, a Knights of Old cresceu e tornou-se uma próspera empresa de logística que opera 500 camiões a partir da sua base em Kettering, uma cidade mercantil no coração da Inglaterra. Altamente conceituada pela sua atitude positiva, a empresa enfrentou todos os desafios que surgiram no seu caminho.

Mas nada do que enfrentou ao longo das décadas se comparava ao devastador ataque cibernético que, em 2023, provocaria o colapso histórico da empresa, com a perda de 730 postos de trabalho. Os hackers conseguiram entrar na rede informática da Knights adivinhando a senha fraca de um funcionário. Em seguida, criptografaram dados importantes e bloquearam todos os sistemas internos, impossibilitando o acesso a informações críticas para o funcionamento diário da empresa.

O ataque foi atribuído a um grupo russo de cibercriminosos conhecido como Akira, que deixou uma nota de resgate sarcástica, dizendo: "Se está a ler isto, significa que a infraestrutura interna da sua empresa está total ou parcialmente destruída... Além disso, obtivemos uma grande quantidade de dados corporativos antes da encriptação... Vamos guardar as lágrimas e o ressentimento para nós mesmos e tentar construir um diálogo construtivo."



Empresas comprometidas

Os hackers exigiram 5 milhões de libras (5,77 milhões de euros) para não publicar os dados corporativos e de clientes roubados na web. A empresa-mãe da Knights of Old, a KNP Logistics, disse que não tinha como conseguir essa quantia. Foram feitos esforços para operar manualmente, mas os danos aos dados críticos e aos sistemas de backup tornaram impossível cumprir os prazos de relatórios financeiros estabelecidos pelos credores e as obrigações de entrega aos clientes. Três meses depois, a KNP entrou em administração judicial.

"Sentíamos que estávamos numa posição muito boa em termos de segurança, protocolos e medidas que tínhamos tomado para proteger o negócio", afirmou o antigo diretor da Knights, Paul Abbot. "Mas, independentemente do que penses que fizeste, pede a opinião de especialistas. As pessoas acham que isso não vai acontecer com elas, mas há centenas de empresas por aí a serem comprometidas. A questão não é apenas o custo, é também o dano à reputação."

Os ataques de ransomware aumentaram mais de 70% no Reino Unido nos últimos anos, tornando-o o segundo país mais visado do mundo, depois dos Estados Unidos. Dados do governo britânico também mostram que, apenas nos últimos 12 meses, pouco mais de 43% das empresas relataram violações ou ataques à segurança cibernética (612.000 no total).

Entre elas estavam as gigantes do retalho M&S, Co-op e Harrods, que foram forçadas a interromper as atividades online por várias semanas enquanto lidavam com as consequências.

A M&S estimou que a interrupção custaria 300 milhões de libras (345 milhões de euros) em lucros perdidos. Das três retalhistas, apenas a Co-op afirmou categoricamente que não havia cedido à exigência de resgate.

E parece que a maioria das empresas paga. A empresa de cibersegurança Sophos descobriu que 54% das vítimas de ransomware no Reino Unido pagaram para recuperar os seus dados nos últimos 12 meses. Normalmente, cada uma entregou 103% da exigência original, muito acima da média global de 85%.

Pagamentos desencorajados

O pagamento de resgates é desencorajado pelo Centro Nacional de Segurança Cibernética (CNSC) e seus parceiros responsáveis pela aplicação da lei, que enfatizam:

- Não há garantia de que terá acesso aos dados ou computador;
- O computador continuará infetado;
- Estará a pagar a grupos criminosos;
- É mais provável que seja alvo de ataques no futuro.

Para reduzir as consequências dos ataques, as empresas são incentivadas a fazer backups offline regulares de ficheiros e dados importantes... especialmente as PME, que estão cada vez mais a ser vítimas das artes obscuras dos hackers.

De facto, os roubos de dados de PMEs mais do que duplicaram no Reino Unido ao longo do último ano, de acordo com o inquérito Cyber Security Breaches Survey 2025 do governo.

Pouco mais de 42% das pequenas empresas e 67% das médias empresas relataram ter sido alvo de um ataque cibernético ou outra violação de segurança durante o período.

As violações cibernéticas podem ser dispendiosas em termos de tempo e perturbações, para além de qualquer pagamento de resgate efetuado. As micro e pequenas empresas, por exemplo, pagam em média 7960 £ (9161 €) para restaurar ou reconstruir os seus sistemas informáticos danificados após uma invasão. Esse valor sobe para 12 560 £ (14 456 €) para as médias empresas. No total, o custo das violações para as PME ascende a cerca de 3,4 mil milhões de libras (3,9 mil milhões de euros) por ano.

Talvez sem surpresa, a inteligência artificial (IA) foi a questão número um para os proprietários de PMEs, com 63% a afirmar que estavam "preocupados" com o crescimento meteórico e a sofisticação crescente da tecnologia. A maioria dos inquiridos (86%) também relatou que a sua empresa tinha sofrido incidentes de segurança relacionados com IA nos últimos 12 meses. Mas apenas 45% estavam confiantes de que a sua empresa estava equipada para realizar avaliações de segurança abrangentes de IA.

A IA reduz a barreira para que cibercriminosos novatos, hackers contratados e hacktivistas realizem operações eficazes de acesso e recolha de informações", informou o Centro Nacional de Cibersegurança no início deste ano. "Isso introduz um novo nível de ameaça cibernética, especialmente para empresas menores que podem não ter o software necessário para mitigar ataques dessa sofisticação."

A segunda maior preocupação em matéria de cibersegurança para os líderes das PME centrou-se no trabalho remoto ou híbrido. Embora os funcionários apreciem ter mais flexibilidade nas suas vidas diárias, o trabalho fora do escritório levanta questões críticas de segurança de dados. No entanto, 69% das PME admitiram não ter uma política de cibersegurança personalizada para os seus trabalhadores remotos.

Quando questionados sobre as medidas de segurança que têm em vigor, 52% dos empregadores afirmaram que utilizam redes privadas virtuais (VPNs), que permitem às organizações fornecer conectividade segura entre dispositivos em locais fisicamente separados. Outros (48%) afirmaram que dão formação aos funcionários sobre trabalho remoto seguro e 46% referiram ter implementado políticas e controlos de acesso remoto.

Dê passos simples

Mas, apesar do cibercrime estar num nível recorde, a pesquisa descobriu que um número significativo de PMEs não tinha barreiras eficazes contra o acesso não autorizado à rede. Isso pode ser porque os empregadores não sabem como manter as suas empresas seguras... ou simplesmente negam a extensão da sua vulnerabilidade a ataques, conclui o estudo.

Agora, o regulador independente do Reino Unido para a proteção de dados está a exortar as PME a "tomarem medidas simples" para reforçar a sua cibersegurança e proteger as informações pessoais que detêm. O Gabinete do Comissário de Informação (ICO - Information Commissioner's Office) afirmou ter recebido relatos de mais de 3000 violações cibernéticas em 2023, a maioria proveniente dos setores financeiro, retalhista e educativo. Num exemplo, foi instalado malware nos terminais de pagamento de um retalhista, permitindo que um hacker recolhesse os dados dos cartões dos clientes enquanto estes efetuavam transações. Noutra ocasião, um simples e-mail de phishing comprometeu as informações pessoais de mais de 100000 trabalhadores da construção civil.

A Information Commissioner's Office (ICO) utiliza estudos de caso para promover o seu relatório "Aprendendo com os erros dos outros", que oferece conselhos práticos para ajudar as organizações a compreender falhas de segurança comuns e a tomar medidas simples para melhorar as suas defesas cibernéticas, com o objetivo de "prevenir futuras violações de dados antes que elas aconteçam".

"As pessoas precisam de se sentir confiantes de que as organizações estão a fazer tudo o que podem para manter as suas informações pessoais seguras", afirmou o vice-comissário da ICO, Stephen Bonner. "Embora os ciberataques estejam a tornar-se cada vez mais sofisticados, constatamos que muitas organizações não estão a responder de forma adequada e continuam a negligenciar os fundamentos da cibersegurança. Como regulador da proteção de dados, queremos apoiar e capacitar as organizações para que façam isso corretamente."

Controlos essenciais

"Embora não exista uma solução única para prevenir ataques cibernéticos, não há absolutamente nenhuma desculpa para não implementar os controlos básicos. Estes são essenciais para proteger as informações pessoais das pessoas, e tomaremos medidas, incluindo multas, contra as organizações que ainda não estão a tomar medidas simples para proteger os seus sistemas. Se sofrer um ataque cibernético, incentivamos sempre a transparência, pois os seus erros podem ajudar outra organização a evitar uma violação semelhante."

Um estudo da British Telecom (BT) revela que 39% das PME – dois milhões de empresas – não oferecem formação em cibersegurança às suas equipas. Em resposta, a gigante das comunicações está a oferecer formação dedicada à sensibilização para ajudar as empresas a compreender as medidas práticas que podem tomar para se protegerem.

A formação também aborda ameaças de última geração decorrentes da IA e da computação quântica. Além disso, destaca atividades criminosas como invasões de contas – em que credenciais roubadas de clientes são usadas para violar sistemas – e golpes com códigos QR (ataques "quishing"), que aumentaram 1400% no Reino Unido nos últimos cinco anos.

"Para as PME, um ataque cibernético não é apenas um inconveniente, mas sim uma ameaça existencial", afirmou Tris Morgan, diretor-geral de segurança da BT. "Uma cibersegurança eficaz não requer recursos de nível empresarial. Com a formação adequada, medidas de segurança básicas e uma maior sensibilização, as PME podem reduzir drasticamente o seu perfil de risco. O segredo está em reconhecer que, no panorama digital atual, a cibersegurança não é um luxo, mas sim uma base que permite às empresas olhar para o futuro com confiança, em vez de estarem sempre a olhar por cima do ombro."

Artigo Original aqui