DICA 1 | janeiro 2022

TEMA	COMO SABER SE FOI HACKEADO

As pequenas e médias empresas (PMEs), pela sua própria natureza, estão em desvantagem quando se trata de combater os ciberataques. O facto de serem pequenas empresas significa que provavelmente não dispõem das mesmas equipas de TI que as grandes empresas, ou dos orçamentos necessários para as proteger do número cada vez maior de ataques. O simples facto de não terem os recursos disponíveis e, por conseguinte, terem uma segurança menos robusta, coloca as PMEs em desvantagem para prevenir e mitigar um ciberataque.

Segundo o Untangle 2021 SMB IT Security Report, as principais barreiras à cibersegurança para as PMEs são os colaboradores que não seguem diretrizes (28% dos inquiridos) e o orçamento (27% dos inquiridos).

Enquanto as grandes empresas têm os recursos necessários para detetar uma violação, as empresas mais pequenas com menos medidas de deteção e segurança em vigor confiam em si próprias e nos seus colaboradores. Ser capaz de reconhecer atividades suspeitas pode ajudar as PMEs a detetarem o ataque e minimizar os danos.

As empresas devem procurar os seguintes indicadores para identificarem um ataque:

1. MENSAGENS DE RANSOMWARE

Esta pode ser a notificação mais óbvia de que foi "pirateado" e infelizmente significa que os seus dados foram encriptados e corre o risco de ser mantido "refém" dos atacantes, a menos que os pedidos de ransomware sejam satisfeitos. A maioria das vítimas acaba com muitos dias de inatividade e tem de adotar passos adicionais de recuperação, mesmo que pague o valor pedido.

2. COMPUTADOR MAIS LENTO OU UMA BATERIA QUE SE ESGOTA RAPIDAMENTE

Se a bateria começar a esgotar-se rapidamente ou o seu computador começar a falhar ou a funcionar muito lentamente, é mau sinal. Pode ser um software malicioso a ser executado de forma invisível, tornando o seu computador mais lento e drenando a bateria.

3. MUDANÇAS SUSPEITAS EM FICHEIROS

Se notar que os ficheiros foram subitamente apagados sem motivo, ou que os nomes de documentos ou pastas foram aleatoriamente alterados, isto pode ser o trabalho de um hacker e deve ser investigado imediatamente.

4. OS PROGRAMAS ANTIVÍRUS OU ANTIMALWARE ESTÃO DESACTIVADOS

O seu antivírus ou outro software de segurança foi subitamente desligado? Pode ser um sinal de que foi comprometido com software malicioso.

5. AS PASSWORDS DE REPENTE NÃO FUNCIONAM

Se tiver a certeza de ter introduzido a palavra-passe correta e ainda não estiver a funcionar, poderá ser vítima de um hacker que acedeu à sua conta e alterou a palavra-passe.

6. INSTALAÇÕES NÃO DESEJADAS

Barras de ferramentas de browser desconhecidas e/ou software instalado no seu computador não são apenas sinais de que foi ATACADO, mas podem abrir ficheiros maliciosos e libertar malware, desativar o seu antivírus, e causar mais alterações indesejadas.

7. OUTRA ACTIVIDADE INVULGAR

• As pesquisas na Internet são redirecionadas

• O ponteiro do rato faz um movimento claro entre programas e faz seleções

• Tentativa de acesso durante horas estranhas ou a partir de locais desconhecidos

• Pop-ups frequentes e aleatórios

As PMEs já se encontram em desvantagem em cibersegurança com orçamentos e equipas mais pequenas.

Para além da monitorização dos sinais acima referidos, aqui estão as medidas que cada empresa pode tomar para se proteger:

• Formar continuamente as equipas. Como os hackers encontram novas formas de se infiltrarem nas redes, manter os colaboradores formados e atualizados só irá reforçar a segurança da sua rede.

• Use autenticação multifator para fornecer uma camada adicional de proteção de dados sensíveis.

• Faça uma cópia de segurança dos seus dados. Se os seus dados forem objeto de backup, mesmo que a sua rede seja violada, um backup pode reverter a máquina para os dados que tinha na véspera do ataque, minimizando as perdas.

• Segmente a sua rede para diferentes tipos de utilização e papéis. Por exemplo, tenha uma rede de convidados que esteja separada da rede principal.

• Mantenha o software atualizado e instale todos os patches de software de forma expedita para evitar uma quebra.

Fique seguro!