Temática: Conhecer a cibersegurança

O que é a cibersegurança?

A cibersegurança, também conhecido como segurança digital, é a prática de proteger as suas informações digitais, dispositivos e recursos. Tal inclui as suas informações pessoais, contas, ficheiros, fotografias e até mesmo o seu dinheiro.

CIA
O acrónimo "CIA" é frequentemente utilizado para representar os três pilares da cibersegurança.

Confidencialidade - Manter os seus dados secretos e garantir que apenas as pessoas autorizadas podem aceder aos seus ficheiros e contas.

Integridade - Garantir que as suas informações permanecem intactas e que ninguém insere, modifica ou elimina os seus dados sem a sua permissão. Por exemplo, alterar mal intencionadamente um número numa primeira vez.

Acesso - Garantir que pode aceder às suas informações e sistemas quando precisar. Um exemplo de um problema de acesso seria um ataque denial of service, em que os atacantes sobrecarregam o seu sistema com o tráfego de rede para que o acesso seja praticamente impossível; ou um ransomware que encripta o sistema e o impede de utilizá-lo.

A segurança é um processo e não um produto
Apesar de as aplicações e dispositivos de segurança, como o software antimalware e as firewalls, serem essenciais, não chega instalar essas ferramentas e ficar descansado. A segurança digital exige a implementação de um conjunto de práticas e processos ponderados. Estes incluem:

- Cópias de segurança de dados - os dados importantes devem ser armazenados numa localização segura, e deverá ser capaz de restaurar uma cópia válida e testada desses dados, caso aconteça algum percalço.

- Bons hábitos digitais – Não abra ligações ou anexos inesperados que possa receber por e-mail ou SMS, mesmo que pareçam ser provenientes de um remetente de confiança.

- Mantenha o seu software atualizado – os sistemas operativos como o Windows, MacOS, iOS ou Android, bem como aplicações e browsers, devem ser atualizados com as correções e correções mais recentes do fabricante.

- Utilizar palavras-passe seguras, exclusivas – as palavras-passe boas devem ter, pelo menos, 14 carateres, não devem ser palavras inglesas e não devem ser reutilizadas em múltiplas contas.

- Utilize a Autenticação Multifator - Sempre que possível, tanto em casa como no trabalho, ative a autenticação multifator para manter as suas contas mais seguras.

- Bloqueie os seus dispositivos - Certifique-se de que os seus dispositivos necessitam de uma palavra-passe, PIN ou autenticação biométrica, como um reconhecimento de impressão digital ou facial, para iniciar sessão. Os dispositivos perdidos ou roubados podem ser uma mina de ouro para os criminosos, caso consigam aceder

facilmente aos dados a partir de um dispositivo desbloqueado.

A cibersegurança é um desporto de equipa

Se vir algo suspeito ou desconfiar que poderá ter sido vítima de acesso ilícito, contacte um consultor de confiança. Se estiver no trabalho ou na escola, comunique essa situação ao departamento de TI da sua organização o mais depressa possível. É possível que seja um falso alarme. No entanto, o seu administrador de TI preferirá certamente ficar descansado ao constatar que se tratava efetivamente de um falso alarme do que ficar alarmado ao detetar um problema, sem que ninguém o tenha comunicado.

Não se iniba de partilhar boas práticas, sugestões ou recursos de segurança que considere úteis com os seus familiares e amigos. Sem forem proveitosos para si, é provável que também o sejam para outras pessoas.

Fonte: Adaptado de support.microsoft.com – 20.Jun.2022.

7 tipos de ataques de hackers que a sua empresa pode sofrer

Uma das grandes preocupações das empresas é serem vítimas de uma invasão mal intencionada. Cada vez mais temos assistido a um aumento dos ataques de hackers, devido à grande quantidade de informações confidenciais que as empresas possuem.

Fique a conhecer 7 ataques de hackers que a sua empresa pode sofrer:

1 - Ransomware

O ransomware tem como objetivo bloquear o acesso a todos os arquivos do servidor, e apenas serão libertados após o pagamento de uma quantidade grande de dinheiro, sendo que o valor do "resgate" será sempre definido pelo próprio criminoso.

Com este ataque, o hacker passa a ter total controlo dos arquivos e informações da sua empresa, e uma vez que os controla remotamente, fica ainda mais difícil de identificar o problema.

Os cibercriminosos fazem com que o utilizador clique num link e instale no seu computador um virus. Este link parece bastante credível, o que leva a que as pessoas não suspeitem de nada.

2 - Phishing

O phishing é geralmente realizado em forma de e-mail, em que os cibercriminosos fazem com que os utilizadores, sem saberem que estão a ser apanhados pelos cibercriminosos, revelem informações confidenciais como passwords e dados bancários, entre outras.

3 - Port Scanning Attack

Este malware o que faz é procurar no servidor vulnerabilidades no sistema de segurança. Se receber alguma mensagem em que existe uma "porta" disponível, este malware irá explorar tudo e poderá ter acesso aos arquivos que estão no servidor.

4 - DDoS Attack

Este ataque tem como objetivo sobrecarregar as atividades do servidor de um computador, fazendo com que fique lento e não consiga aceder aos sites.

Quando um site fica indisponível, os utilizadores não irão conseguir aceder ao seu site, o que poderá originar perda de vendas ou não conseguirem aceder aos seus serviços.

5 - Cavalo de Troia

Esta é uma das ameaças mais conhecidas, e este malware só irá funcionar com a "autorização" do utilizador. Para que isto aconteça, o utilizador clicou por exemplo em algum anexo que veio num email suspeito ou desconhecido.

Existem vários objetivos que os cibercriminosos pretendem objetar com este malware: roubar informações pessoais ou parar algumas funções do seu computador.

6 - Ataques de força bruta

Este ataque consiste no furto de passwords através de diversas tentativas de combinação de utilizador e password. Quando os cibercriminosos tiverem esta informação, poderão enviar diversas mensagens, em que o remetente é conhecido, com conteúdos como phishing e spam.

7- Ataques internos

Os ataques desta natureza, podem ser realizados por pessoas mal intencionadas. Estes ataques internos podem ser feitos por pen's infectadas, instalações de sistemas, uso de malwares nos computadores ou inúmeras situações prejudiciais.

Fonte: Adaptado de Artigos inovflow.pt – 20.Jun.2022.