Laboratório – Que dados foram roubados?

Objetivos

Pesquise e leia acerca de algumas ocorrências de falhas de segurança recentes.

Contexto/cenário

As falhas de segurança ocorrem quando indivíduos ou aplicações tentam obter acesso não autorizado a dados, aplicações, serviços ou dispositivos. Durante estas falhas, os atacantes, quer sejam elementos internos ou não, tentam obter informações que podem utilizar para ganhos financeiros ou outros proveitos. Neste laboratório, irá explorar algumas falhas de segurança para determinar o que foi roubado, os exploits que foram utilizados e o que pode fazer para se proteger.

Recursos necessários

- PC ou dispositivo móvel com acesso à Internet

Pesquisa de falhas de segurança

a. Utilize as três ligações fornecidas para verificar a existência de falhas de segurança em setores diferentes para preencher a tabela abaixo.

b. Pesquise algumas outras falhas interessantes e registe os resultados na tabela abaixo.

Data do incidente	Organização afetada	Quantas vítimas? O que foi roubado?	Que exploits foram utilizados? Como pode proteger-se?	Fonte de referência
30/03/2022 02:00 da manhã	Sonae	Clientes da SONAE, SONAE. Ficaram comprometidos os dados dos clientes	Os exploits que foram utilizados foi o phishing. Ter conhecimento de técnicas de cibersegurança para poder prevenir	Jornal Público
26/08/2022	TAP	foi Roubado material confidencial / dados pessoais 1.5 milhões de pessoas	exploits usado foi phishing Ter conhecimento de técnicas de cibersegurança para poder prevenir	CNN Portugal
07/02/2022 ao final da noite	Vodafone	foram Roubados dados pessoais de alguns clientes como nome, morada. Cerca de 4 milhões de pessoas.	Técnico defendeu a informação explicitamente	Jornal DN

Reflexão

Depois de ler acerca destas falhas de segurança, o que pode fazer para impedir estes tipos de falhas?

Depois de ler acerca destas falhas de segurança relativas aos sistemas informáticos, sobre a SONAE, Vodafone e TAP o que se pode fazer para impedir este tipo de ataques são, criptografar dados sensíveis, fazer backup Regulares de todos os dados, avaliação de segurança regularmente feitos por especialistas na área e gerenciar os incidentes.