

CIBERATAQUE

Olá! Você é daquelas pessoas que tapa a senha do seu cartão de crédito quando vai pagar? E... também é daquelas pessoas que tapa a webcam de seu computador? Sim? Parabéns! É isso o que você tem que fazer; é muito importante.

E então: por que você abre e-mails vindos de destinatários desconhecidos? Tanto a nível particular quanto em uma rede corporativa de sua empresa, você deveria ficar alerta porque em qualquer momento pode receber uma visita indesejada... a de um pirata informático.

O podcast para aqueles que querem mudar o mundo. É o momento de pensar no futuro do planeta. O que você tem que saber sobre... os ataques cibernéticos?

(intro)

Em pleno século XXI, o século da digitalização, a tecnologia progride com passos gigantescos. Os progressos em termos de inteligência artificial, big data ou da Indústria 4.0 também têm seus argumentos contrários . A Internet é vulnerável e os ciberataques põem em cheque a informação de particulares , empresas e países inteiros. De fato, segundo o especialista em política tecnológica e desenvolvimento digital Alec Ross:

<https://www.iberdrola.com/shapes-pt/alec-ross-ciberconflitos-que-definirao-os-proximos-cinco-anos>

Os progressos em ciberdelinquência têm custos espetaculares. Prevê-se que em 2021 o custo total da delinquência informática chegue a 6 bilhões de dólares. Esta cifra aumentará para mais de 10 bilhões de dólares em 2025, o que faz da delinquência informática um dos problemas e desafios mais importantes para as empresas e a sociedade nos próximos anos.

O que são exatamente os ciberataques? O que eles significaram para o progresso da humanidade?

(som de teclado, de senha errada)

Um ataque cibernético é um conjunto de ações contra os sistemas de informação (tais como bases de dados) com o objetivo de prejudicar pessoas e organizações. O objetivo é anular

serviços, espiar ações de concorrentes, roubar informação e, inclusive, extorquir a própria instituição.

A espionagem e o roubo de informações são uma coisa intrínseca da existência humana. Têm ocorrido inúmeros ataques contra os sistemas de comunicação mais modernos: desde se preparar contra invasões inimigas até um vírus no servidor da multinacional mais atualizada em termos de proteção.

(som de máquina de tempo/viagem no tempo, tom curiosidade) Ano 1940-1942

O mais conhecido enigma da Segunda Guerra Mundial foi decifrado pelo matemático Turing. Com a criação da máquina “Bomba”, ele descodificou o código Enigma, a criptografia criada pelo lado alemão. Esta descodificação ajudou as potências aliadas a vencerem a guerra.

(som de máquina de tempo/viagem no tempo, tom curiosidade) Ano 1834

Porém, o primeiro ciberataque do qual temos constância se relaciona com o telégrafo óptico, um inovador sistema de comunicação utilizado pelo governo francês. Até que chegaram os irmãos Blanc.

Estes dois banqueiros queriam aproveitar o sistema para ser os primeiros em conhecer a situação do mercado francês, informação que demorava vários dias em chegar desde a capital do país. Subornaram um técnico que escondia, entre as mensagens do governo, o valor dos bônus franceses, captados instantaneamente por um ajudante dos irmãos. O ciberataque da época durou mais de dois anos.

(som de máquina de tempo/viagem no tempo, tom curiosidade) Os anos de 2010

Os ciberataques têm deixado rastros em grande escala nos últimos anos, gerando conflitos econômicos e pânico social.

Em 2008, um malware se infiltrou nos sistemas vulneráveis do Windows, infectando 10 milhões de equipamentos em 190 países. Em 2010, o Irã e outros países sofreram ataques cibernéticos em suas infraestruturas críticas, o que causou temor a uma agressão nuclear a estes países. Em 2017, uma grande quantidade de computadores europeus teve seus arquivos encriptados e todos seus acessos bloqueados. Milhares de empresas ficaram paralisadas por um malware muito descritivo: “wannacry”.

(som de máquina de tempo/viagem no tempo, tom curiosidade) Ano 2021

Atualmente, é mais provável que tenhamos antes uma guerra cibernética do que uma tradicional. É o que indica Keren Elazari, especialista em segurança cibernética e cultura hacker com várias conferências TED em seu currículo.

<https://www.iberdrola.com/shapes-pt/keren-elazari-ciberguerra-no-contexto-de-conflitos-globais>

Na era da ciberguerra, tanto as nações quanto as empresas reconceberam as linhas de batalha: agora elas são virtuais. Esta era começou há aproximadamente dez anos, quando um vírus informático chamado Stuxnet mudou as regras do jogo. Foi a primeira arma cibernética do mundo: um código informático capaz de alterar instalações físicas. No contexto da geopolítica, uma arma digital como o Stuxnet poderia ser entendido simplesmente como o método mais conveniente, não violento e rentável para interromper de forma encoberta um programa de armas nucleares.

Já existem várias organizações criminais orientadas aos ciberataques. De fato, durante a pandemia, aumentaram sua atividade em 25 %. Sua alta rentabilidade e a dificuldade de rastreamento são muito apetecíveis para os piratas cibernéticos.

(explicativo e enumerativo)

Há diversos tipos de ciberataques, conforme sua execução, finalidade, a vítima...

(fazendo um aparte) Vamos descobri-los ajudados pela Kaspersky, empresa líder em cibersegurança

- Phishing. Envio de mensagens fraudulentas que aparentemente procedem de fontes confiáveis e seguras. Utiliza-se especialmente em e-mails. O objetivo é roubar dados pessoais como inícios de sessão ou informações bancárias.
- Malware. Software malicioso com vírus e malwares. Seu impacto vai desde a instalação de um programa danoso para o bloqueio de acesso a componentes da rede (ransomware) até a obtenção de informações (spyware).
- Injeção de SQL (SQL injection). Um hacker insere um código malicioso em um servidor que utiliza linguagem de consulta estruturada, revelando informações protegidas.

- Ataque de recusa de serviço. Satura sistemas, servidores e inclusive redes com tráfego para esgotar seus recursos e a largura de banda.

(explicativo)

Para se proteger desses ciberataques, você precisa de uma rede de segurança cibernética. Este sistema detecta, identifica e detém ameaças de forma rápida, criando um perímetro de segurança. Controla quem entra em sua rede e protege todos os dispositivos vinculados à sua rede, tanto doméstica quanto profissional.

(enumerado e prático, efeitos sonoros relacionados com cada enumeração)

No entanto, você também pode ajudar a prevenir esses ataques no seu cotidiano na Internet:

- Atualize seus equipamentos e programas antivírus. As últimas melhorias corrigem falhas de segurança das versões anteriores.
- Use senhas longas e complexas. Que não sejam sempre as mesmas nem incluam informação facilmente decifrável, como seu aniversário ou animal de estimação.
- Não clique em links suspeitos. Os servidores da Internet costumam avisar quais são os sites não seguros.
- Não proporcione dados pessoais para sites desconhecidos ou pouco confiáveis. Confie só em espaços seguros e oficiais.
- Denuncie às autoridades qualquer website, link ou e-mail duvidoso.

Os ciberataques avançam mais rápido que a própria tecnologia e a digitalização. Embora sua detecção esteja nas mãos de organismos nacionais e internacionais, é nossa responsabilidade dificultar ao máximo sua expansão, sendo consumidores inteligentes da rede de redes.

Obrigado por se preocupar pelo futuro. Agora, devemos passar à ação. Continue descobrindo boas iniciativas para o planeta no seguinte podcast, em suas plataformas favoritas ou nas seções de inovação e sustentabilidade da Iberdrola.com