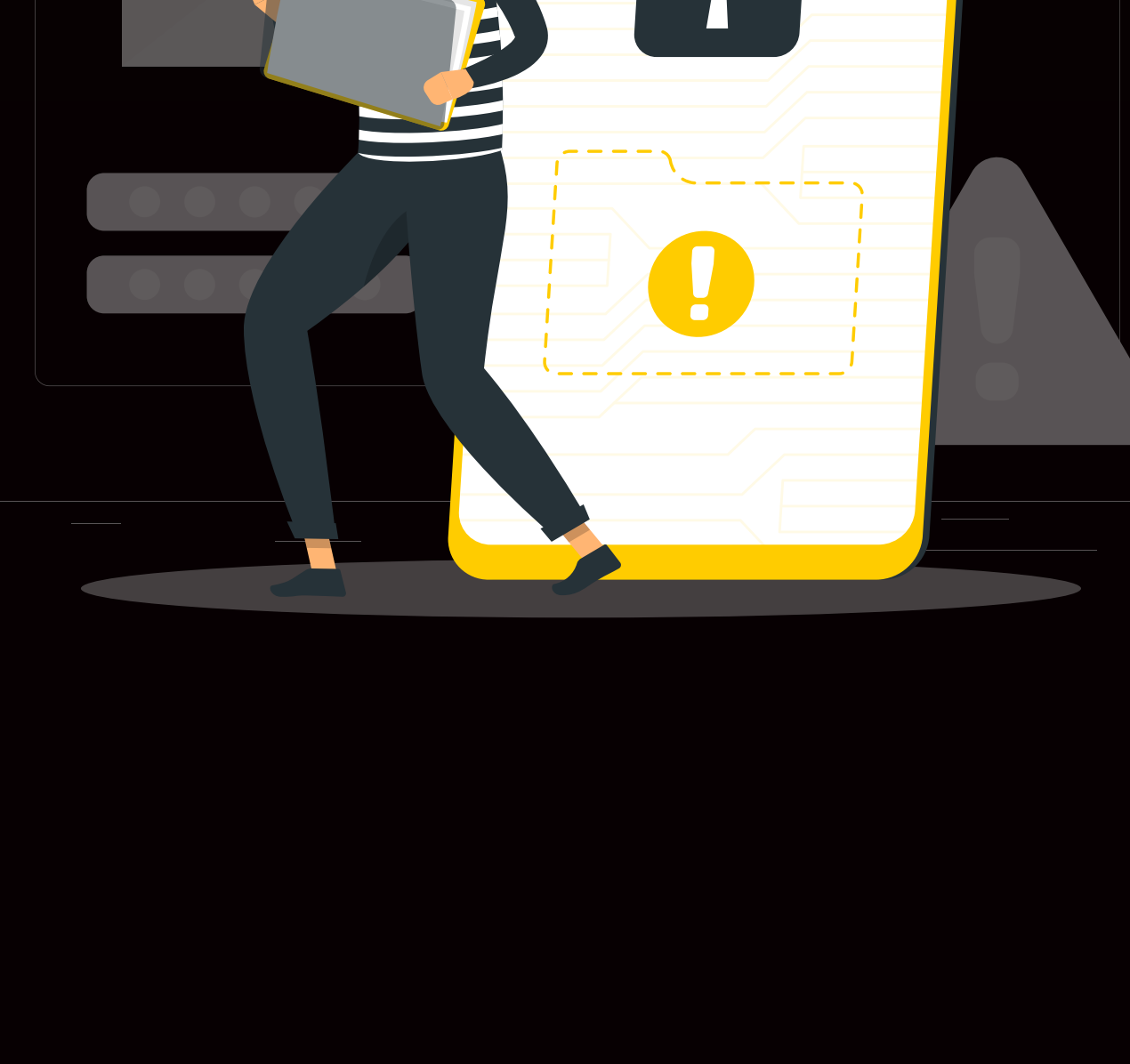


5 ATAQUES CIBERNÉTICOS

mais comuns nas empresas e como proteger seu negócio deles

Não é novidade alguma que o número de ataques cibernéticos tem crescido. Para saber contra o que está se lutando, descubra mais abaixo cinco dos ataques mais comuns e como se proteger.



OS NÚMEROS NÃO MENTEM

Para demonstrar como os ataques cibernéticos interferem no cotidiano das empresas, nada melhor do que números. Para tanto, estudos de marcas reconhecidas no mercado de tecnologia:

Aumento de **72%**

na média de casos de **RANSOMWARES**

no primeiro semestre

de 2020 (Skybox Security)

Aumento de mais de

300%

em **Ataques** no Brasil

com o início da crise

sanitária (Kaspersky)

Garmin teve prejuízo de

10Mi

de dólares em julho

devido ao sequestro de

dados (BleepingComputer)

Ameaças de segurança, como sequestro de thread e ataques de whaling, **devem crescer ainda mais em 2021** (HP)

Nos próximos meses

os ataques devem se

direcionar à usuários

e endpoints (HP)

ATAQUES CIBERNÉTICOS MAIS COMUNS NO AMBIENTE CORPORATIVO



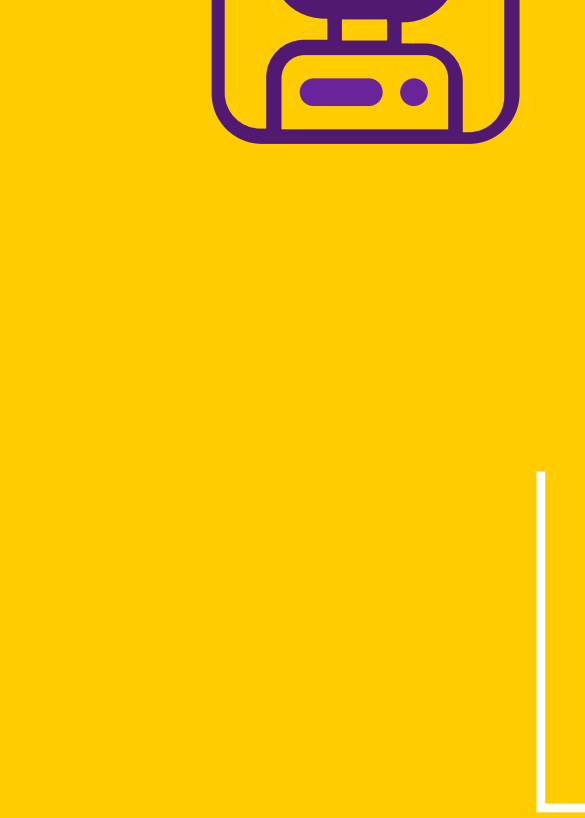
RANSOMWARE

O Ransomware, também conhecido como sequestro de informações, busca, por meio de softwares, bloquear o uso dos dados empresariais até que a empresa pague para "resgatá-los"



PHISHING

Técnica de engenharia social em que o hacker envia links maliciosos, geralmente muito semelhantes a sites que o usuário acessa com frequência, a fim de solicitar e roubar dados.



ATAQUES DE FORÇA BRUTA

Esses ataques são promovidos por robôs que tentam uma infinidade de logins e senhas. Assim, em certo momento, os hackers acertam os dados, conseguindo acesso total à central da organização.



BACKDOOR

Ataques backdoor são trojans que entram nos computadores por meio da instalação softwares e hardwares de origem duvidosa, para que o invasor possa controlar as ações e roubar dados no sistema.



ATAQUE DDOS

Apesar de não ter o objetivo de roubar dados, o DDoS, que visa sobrecarregar atividades de um servidor e paralisar operações de empresas, é um dos ataques mais comuns e difíceis de se perceber, principalmente com a popularização do trabalho remoto.

COMO PREVENIR SUA EMPRESA DE ATAQUES DE HACKERS?

UTILIZE APENAS SOFTWARES OFICIAIS

Utilize sempre softwares e aplicativos oficiais. Arquivos de programas da internet ou de fontes duvidosas podem infectar seu computador ou toda rede empresarial.

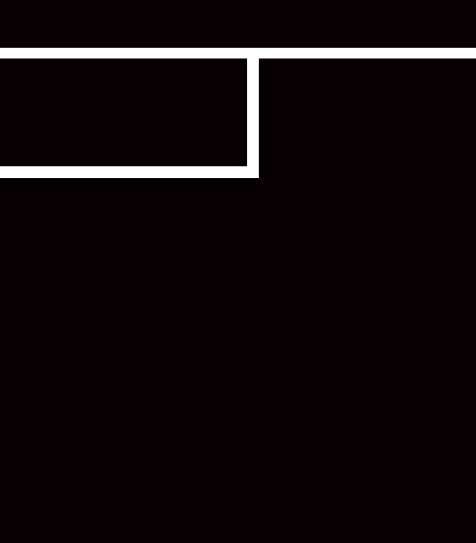


MANTENHA OS SISTEMAS ATUALIZADOS

Mantenha os gadgets da companhia sempre atualizados com a mais recente versão do sistema. Afinal, as novas versões disponibilizadas pelo fabricante dificultam a entrada de hackers.

TREINE SEUS COLABORADORES

Em um cenário em que maior parte dos ataques se inicia a partir da engenharia social, políticas de segurança para preparar os colaboradores podem fechar muitas portas de entrada aos seus banco de dados.



DEFINA SENHAS FORTES

Mantenha os gadgets da companhia sempre atualizados com a mais recente versão do sistema. Afinal, as novas versões disponibilizadas pelo fabricante dificultam a entrada de hackers.

CRIE UMA ROTINA DE BACKUP

Tenha sempre uma cópia de segurança de todos os dados da companhia. De preferência, mantenha os dados em um servidor externo.



UTILIZE FERRAMENTAS DE SEGURANÇA

Invista em ferramentas de monitoramento e proteção, como firewalls, antivírus e criptografia. Instale-as em toda a estrutura da companhia e mantenha uma análise sobre seus resultados.

PROTEJA SEUS DADOS COM A STORAGEONE

Com todos esses dados mostrados acima, fica evidente que é preciso **se proteger contra os ataques cibernéticos**. Mas, para isso, o ideal é contar com **parceiros que possuam experiência e qualidade** em seu trabalho.

A **StorageOne** é uma empresa que conta com 20 anos atendendo clientes de diversos segmentos. Com foco na **segurança, desempenho e compliance**, é a parceira ideal para você proteger seus dados e de seus clientes.

Ficou interessado?

Entre em contato com a StorageOne para mais informações.

[Agendar Reunião](#)