BOAS PRÁTICAS EM CIBERSEGURANÇA

OS ATAQUES EVOLUEM E NÓS TEMOS DE EVOLUIR COM ELES

A SUA EMPRESA SOFREU UM ATAQUE POR RANSOMWARE!

E agora sabe o que deve fazer?

PRIMEIRO É NECESSÁRIO PERCEBER O QUE É O RANSOMWARE.

RANSOMWARE

RANSOM = RESGATE

"O ransomware é um tipo de **software malicioso** (ou malware) que ameaça uma vítima ao destruir ou **bloquear o acesso a dados** ou sistemas críticos até que o resgate seja pago. Recentemente, o ransomware operado por humanos – cujo **alvo são organizações** – tornou-se a **maior ameaça** e a mais difícil de impedir e inverter. Com o ransomware operado por humanos, um grupo de atacantes utiliza a sua inteligência coletiva para aceder à rede empresarial de uma organização. **Alguns ataques deste tipo são tão sofisticados que os atacantes utilizam documentos financeiros internos que expuseram para definir o preço do resgate."**

SEQUESTRADOR DE DADOS

Os alvos são sempre os dados das organizações, e depois dos atacantes invadirem os diferentes ficheiros eles ficam totalmente **INACESSIVÉIS**.

Isto acontece muitas vezes porque alguém da empresa recebe um email e abre um anexo ou clica num link que possui malware (software malicioso). **E o resultado é assustador!**


RANSOMWARE ATTACK
ARE ENCRYPTED

QUAIS OS DANOS PROVOCADOS?

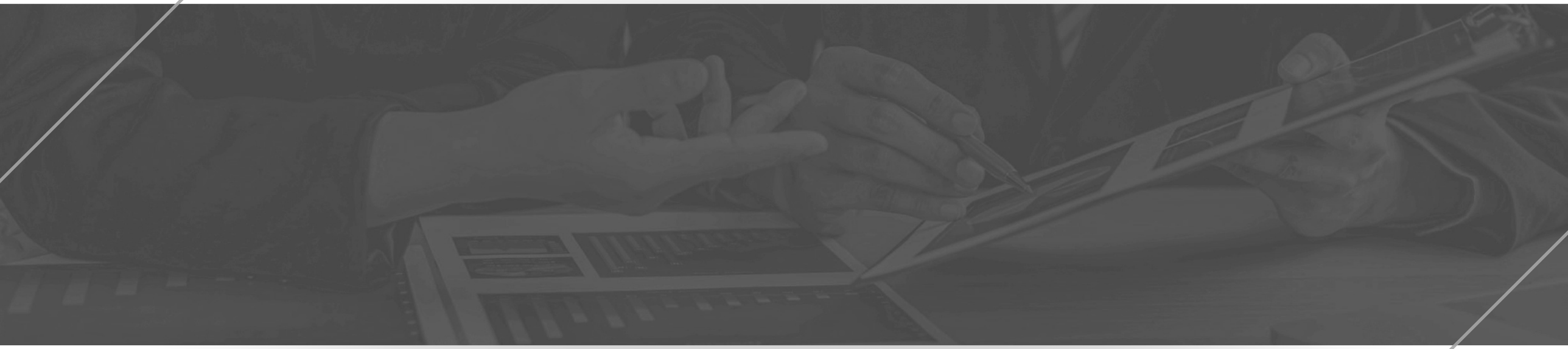
Muitas das vezes acontece o roubo de dados pessoais, bancários e outras informações confidenciais da sua empresa, deixando-a comprometida. Inclusivamente, os dados de clientes podem ficar expostos.

Isto porque todas estas informações valem dinheiro e muitos estão dispostos a comprar. Já para não falar do tempo de paragem do negócio da empresa. **NÃO FATURA**, compromete a rotina de trabalho, atrasos nas entregas.

E isto traduz-se no pedido de resgate de dados, ou seja estamos a falar de muito dinheiro, a maior parte pago em bitcoins ou outro tipo de criptomoeda.
E AGORA?

E AGORA?

É IMPORTANTE PERCEBER QUE NÃO É ACONSELHÁVEL PAGAR O RESGATE!



ISTO PORQUE **91% DAS EMPRESAS** QUE PAGAM O RESGATE **NÃO TÊM** GARANTIA DE RECUPERAR OS SEUS DADOS. E MUITO MENOS DE FORMA INTEGRA, COMO PODEMOS CONFIAR QUE OS DADOS NÃO ESTÃO INFETADOS?

MAS AFINAL COMO PODE PROTEGER A SUA EMPRESA?

O QUE PODEMOS FAZER? COMO PROTEGER A EMPRESA DE ATAQUES DE RANSOMWARE?

Uma vez que o software malicioso se aproveita da vulnerabilidade da infraestrutura e falta de conhecimento técnico dos colaboradores para se instalar na rede e sistemas operativos. Logo é fundamental:

- Investir em ferramentas aliadas da segurança da informação;
- Manter as ferramentas e softwares da empresa atualizados;
- Manter os colaboradores conscientes e com a formação adequada para reforçar o ecossistema seguro da empresa, porque são o primeiro ponto de entrada deste tipo de ameaças;
- Garantir sempre que os computadores, servidores e afins estejam protegidos com robusto software de segurança de endpoint e as políticas de segurança sejam revistas regularmente, bem como ter uma boa firewall.
- Ter backups imutáveis, regulares, seguros à prova de falhas.
- Ter um sistema de monitorização que permita visualizar o estado de todos os dispositivos da rede.

OS ATAQUES EVOLUEM E NÓS TEMOS DE EVOLUIR COM ELES.

NÃO SE QUER PREOCUPAR COM ESTAS QUESTÕES?
Encontre um bom parceiro consultor em tecnologia e especialista em cibersegurança.
Um bom parceiro vai:

- Simplificar a visão, aconselhar e implementar com segurança as melhores soluções.
- Tire 30 minutos para falar com o João Mota, CTO da Quantinfor e esclareça todas as suas dúvidas: https://calendly.com/joaomotaquantinfor/30min

QUANTINFOR

CONSULTORIA INFORMÁTICA

www.quantinfor.com

jmota@quantinfor.com

(+351) 219 668 911

chamada para a rede fixa nacional

in/joaopmota/