Capgemini

SOLUÇÕES ANTI-*RANSOMWARE*

Quando ameaças surgem a todo instante, a segurança tem que ser completa.

***Ransomware*: um complexo problema de *cyber* segurança**

Sistema e arquivos bloqueados. Empresa feita de refém por criminosos. Exigência de pagamento para liberar o acesso. Infelizmente, esse tipo de cenário é cada vez mais comum: são os famosos *ransomwares*, ameaças digitais que fazem vítimas no mundo inteiro.

Conhecendo o inimigo

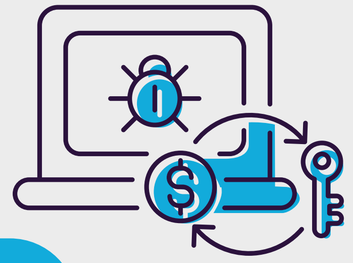
Grupos especializados em bloquear sistemas e extorquir um valor de resgate;

Cada vez mais sofisticados, atuam com o conceito "*ransomware as a service*";

Formados por negociadores, desenvolvedores, *pentesters*, entre outros;

Atingem tanto empresas quanto órgãos públicos.

O ciclo de vida de um *ransomware*



ACESSO
Criminosos invadem o sistema da vítima por meio de técnicas variadas.

DESENVOLVIMENTO
Após o acesso, levantam informações e obtêm acesso remoto ao sistema.

IMPACTO
Com os dados em mãos, podem criptografá-los para extorquir a vítima.

Um grande impacto nos negócios

- Interrupção das atividades da empresa
- Perdas financeiras
- Perda total de dados
- Danos à reputação
- Vazamento de informações sigilosas
- Riscos de sanções regulatórias

Capgemini

AMEAÇA PERIGOSA, SEGURANÇA CONSISTENTE

Sim, os *ransomwares* são um problema sério. Mas temos uma ótima notícia: a *cyber* segurança evoluiu enormemente. Hoje, temos soluções eficientes para manter sua empresa protegida e preparada para o futuro.

Além da *cyber* segurança: *cyber* resiliência

Cyber resiliência é a capacidade de prever, resistir, se recuperar e se adaptar a condições adversas, ameaças cibernéticas e mudanças no mercado. Em um mundo de transformações digitais e trabalho remoto, esse conceito é mais do que uma estratégia: é uma necessidade.

E nós podemos te ajudar com isso.

Como a Capgemini torna sua empresa mais resiliente e segura

Na hora de falar sobre proteção anti-*ransomware*, a primeira coisa que você precisa saber é: não existe bala de prata. Esqueça soluções milagrosas, o que funciona de verdade é uma estratégia holística e completa feita sob medida para o seu negócio.

Conscientização de usuários
Campanhas, exercícios e simulações de incidentes de *ransomware*.

Continuidade de negócios e recuperação
Backups, replicações de dados e revisão de processos críticos.

Resposta a incidentes e gestão de crises
Processos eficientes e ágeis para responder a incidentes operacionais.

Monitoração, detecção e resposta
Rápida identificação e combate a atividades suspeitas.

Capacidades de log e auditoria
Aperfeiçoamento de ferramentas e processos de registro de ações e auditorias.

Segurança e gestão de *endpoints*
Proteção de *endpoints* em home office, na empresa ou na nuvem.

Inventário de ativos
Reforço dos processos de controle de ativos (hardware e software).

Acessos remotos
Avaliação da segurança dos mecanismos de acesso remoto.

Gestão de vulnerabilidades
Escaneamento contínuo da gestão de vulnerabilidades, *patches* e *hardening*.

Identidades e acessos privilegiados
Revisão da gestão de acessos privilegiados (perfis, senhas e autenticações).

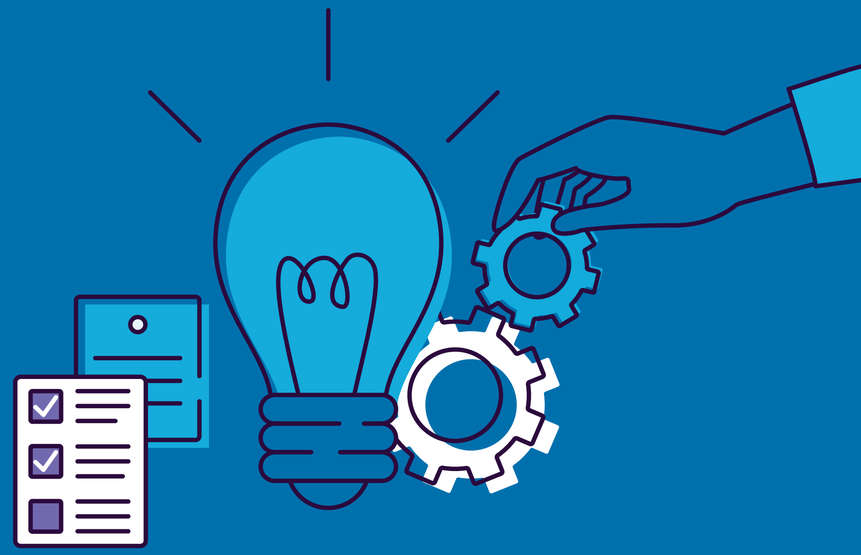
***Pentest* (teste de invasão)**
Ataque simulado ao sistema, incluindo serviços web e APIs.

Capgemini

CAPGEMINI NA PRÁTICA

O plano de trabalho

Agilidade, precisão e praticidade: nosso plano é desenvolvido sob medida para suas necessidades de segurança e pode ser implementado entre 6 e 10 semanas. E pode ficar tranquilo: da abertura ao fechamento, fazemos a gestão completa do projeto.



PREPARAÇÃO	DIAGNÓSTICO	PLANO MESTRE	*QUICK WINS*	FECHAMENTO
Definições iniciais, incluindo estruturas de controle, status do projeto e equipes responsáveis.	Avaliação completa da postura de segurança e da proteção de ativos da sua empresa.	Análise profunda dos resultados do diagnóstico e criação de plano de ação anti-*ransomware*.	Desenvolvimento de medidas de rápida implementação e baixo custo para mitigar riscos de segurança.	Consolidação de todas as entregas e reuniões técnicas e executivas de encerramento do projeto.

Capgemini

SOBRE O PLANO MESTRE

Contém todo o racional por trás da estratégia da Capgemini;

Possui *roadmap* para a evolução da sua segurança no combate a *ransomwares*;

Agrupa as iniciativas de acordo com urgência/rapidez de implementação;

Possui estimativas de prazos e esforços para cada ação;

Apresenta a Ficha de Gestão de Riscos, que registra todo o progresso do projeto.

Revisão da postura de segurança

Avaliação baseada em práticas do mercado reconhecidas internacionalmente, como a ISO 27002 e o NIST CSF. Nossa prioridade é diminuir riscos e impactos a cada fase do ciclo de vida do *ransomware*.

Revisão de ativos

Desenvolvimento de estratégia de proteção e rápida recuperação em caso de ataque, com foco na integridade das operações e nos riscos corporativos.

- Soluções para nuvem, backups, VMware, Microsoft O365 e muito mais;
- Garantia de disponibilidade dos sistemas críticos de TI;
- Criação de *guidelines* para casos de ataques cibernéticos;
- Parceria com fornecedores para combater os *ransomwares*.

Por que escolher a Capgemini?

1. Somos referência de mercado em *cyber* segurança e privacidade;
   a. Líder em Serviços de Gerenciamento de Segurança em TI 2021 pelo PEAK Matrix®, do Everest Group
   b. IDC MarketScape Names Capgemini a Leader in Managed Security Services
2. Expertise local, força global com centros de operações por todo o mundo
3. Mais do que uma consultoria, somos parceiros na sua transformação digital;

Saiba mais sobre nossas soluções de Cibersegurança.
Visite nosso site: www.capgemini.com/br-pt