CIBERSEGURANÇA PARA ORGANIZAÇÕES MAIS PEQUENAS

LISTA DE VERIFICAÇÃO DE RANSOMWARE

PREPARAÇÃO PARA ENFRENTAR O RANSOMWARE

☐ **À medida que desenvolve um plano de prevenção e proteção contra o ransomware, avalie periodicamente o seguinte:**

- A sua organização tem programadas cópias de segurança regulares?
- Quaisquer dispositivos não essenciais estão ligados à rede da sua organização?
- A sua organização compreende os riscos regulamentares e jurídicos envolvidos no pagamento de um resgate?
- A sua organização atualiza regularmente os seus sistemas de software? Estas atualizações são automatizadas?
- A sua organização tem um plano para lidar com um ataque de ransomware e perda de dados?
- O seu sistema tem uma apólice de seguro contra riscos cibernéticos? Em caso afirmativo, como é que esse plano cobre os ataques de ransomware?

PROTEÇÃO EM TEMPO REAL

☐ **Invista em sistemas de proteção anti-malware, que se adaptem às informações sobre novas ameaças em tempo real.**

☐ **Avalie a segurança de todos os dispositivos ligados a redes que contenham informações sensíveis ou essenciais.**

- ☐ Ligue todos os sistemas não essenciais a uma rede separada.
- ☐ Considere a segurança de estações de trabalho remotas. Garante que as ferramentas de segurança trabalham fora da rede para monitorizar todo o tráfego Web.

☐ **Promova a formação dos funcionários em matéria de ataques de phishing e a necessidade de ter proteções de palavras-passe fortes.**

☐ **Considere implementar a autenticação multifator em toda a sua organização, caso tal seja viável.**

☐ **Mantenha todo o software e todos os sistemas atualizados regularmente.**

- ☐ Altere as definições para permitir atualizações automáticas, se possível.

☐ **Desenvolva um plano de resposta a incidentes e gestão de crises para saber como lidar com um ataque de ransomware e a perda de dados valiosos.**

- ☐ Prepare um plano de comunicação externa em caso de um ataque de ransomware.

CÓPIAS DE SEGURANÇA DE DADOS

☐ **Invista em sistemas de cópia de segurança seguros e atualizados regularmente, que mantenham os seus dados protegidos.**

- ☐ Se usar USB ou discos rígidos, desligue fisicamente estes dipositivos dos computadores ligados à rede após a conclusão das cópias de segurança.
- ☐ Se utilizar armazenamento na cloud, equipe os servidores com encriptação de alto nível e autenticação multifator.

☐ **Crie uma cópia de apenas leitura do razão geral, para efeitos de recuperação pós-catástrofe no pior dos casos.**

☐ **Desenvolva sistemas que realizem a recuperação e reparação automáticas de dados.**

☐ **Desenvolva cenários para avaliar quando tempo levará para recuperar dados e serviços empresariais essenciais.**

AMBIENTE REGULAMENTAR

- ☐ **Avalie as orientações regulamentares e jurídicas relevantes em matéria de ransomware no seu ambiente operativo.**
  - ☐ Considere as orientações específicas do país.
  - ☐ Considere as orientações específicas para o setor financeiro
  - ☐ Considere os requisitos jurídicos e regulamentares de âmbito internacional.
  - ☐ Desenvolva um plano para a avaliação periódica de orientações em mudança.
- ☐ Avalie os riscos envolvidos no pagamento de um resgate.
- ☐ Articulação com as autoridades locais de aplicação da lei.
- ☐ Desenvolva ligações para a partilha rápida de informação em caso de um ataque.
- ☐ Avalie as vantagens e desvantagens das apólices de seguro contra riscos cibernéticos, nomeadamente ransomware.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org