Avaliação de cibersegurança: **como manter o seu negócio seguro**

60% das PME encerram nos seis meses seguintes a um ciberataque. Uma avaliação de cibersegurança mostra-lhe o que está a funcionar e, crucialmente, o que não está. Concebida em torno dos “5 Cs da cibersegurança”, a nossa lista de verificação simples de sete passos mostra-lhe o que procurar e como proteger o seu negócio.

vodafone business

1 Defina o âmbito

- Decida que parte do seu negócio está a avaliar – a organização inteira, equipas remotas, cadeia de fornecimento ou um sistema específico.
- Liste as pessoas, processos, tecnologia e terceiros envolvidos.
- Clarifique o que está dentro do âmbito e o que não está, para que nada seja esquecido.

2 Identifique e priorize os seus ativos

- Liste todos os dispositivos críticos para o negócio – portáteis, telemóveis, servidores, routers, etc.
- Inclua plataformas cloud, sistemas de email e software de que a sua equipa depende diariamente.
- Sinalize tudo o que armazena, processa ou acede a dados sensíveis.
- Classifique cada um com base no quão essenciais são ou no quão prejudicial seria perdê-los.

3 Mapeie os riscos

- Identifique ameaças prováveis – phishing, malware, palavras-passe fracas, erro humano, violações na cadeia de fornecimento.
- Para cada ativo, pergunte: qual é o risco? Qual é a probabilidade? Qual seria o impacto?
- Destaque as suas maiores vulnerabilidades – aquelas que provavel mente terão o maior impacto.

4

Reveja as suas proteções atuais

- Verifique se o seu antivírus, firewalls, controlos de acesso e ferramentas de encriptação estão ativos e atualizados.
- Reveja os processos de cópia de segurança de dados e a rapidez com que poderia recuperar de uma perda.
- Avalie a formação dos colaboradores. As suas equipas sabem como reconhecer e responder a ameaças?

5

Reveja o risco de fornecedores e parceiros

- Liste fornecedores, contratantes ou prestadores de serviços com acesso aos seus sistemas ou dados.
- Avalie cada um para verificar se estão a cumprir as suas expectativas de segurança.
- Verifique quaisquer contratos e SLA e certifique-se de que têm requisitos de segurança claros.

6

Crie o seu plano de ação

- Crie uma lista clara e priorizada de correções, começando pelas soluções rápidas e pelos riscos de alto impacto.
- Atribua responsáveis e defina um cronograma para uma responsabilização clara.
- Monitorize o progresso com verificações regulares.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

7

Teste o seu plano de resposta empresarial

- Execute uma simulação ou um ciberataque fictício para descobrir como a sua equipa responde.
- Verifique se o seu plano de incidentes funciona em tempo real para garantir que todos sabem o que fazer, quando fazer e o que acontece a seguir.
- Certifique-se de que as cópias de segurança, listas de contactos e funções de resposta estão atualizadas e acessíveis.
- Ajuste o plano conforme necessário.

Pronto para passar de reativo a proativo?

Os cibercriminosos estão a tornar-se mais sofisticados e as ameaças estão a mudar constantemente, pelo que manter-se um passo à frente é fundamental.
Ao consultar regularmente esta lista de verificação, pode detectar fraquezas precocemente, manter a conformidade e integrar uma melhor proteção nas suas operações diárias.

vodafone business