enisa

AGÊNCIA DA UNIÃO EUROPEIA
PARA A CIBERSEGURANÇA

Guia de cibersegurança para as PME

12 PASSOS

PARA PROTEGER A SUA EMPRESA

A crise da COVID-19 mostrou a importância, em geral, da Internet e da informática para as PME. Para os negócios prosperarem durante a pandemia, muitas PME tiveram de tomar medidas de continuidade das suas atividades, tais como a adoção de serviços na nuvem, a melhoria dos serviços de Internet, a atualização dos sítios Web e a possibilidade de teletrabalho.

Este folheto fornece às PME 12 medidas concretas de alto nível sobre a melhor forma de proteger os seus sistemas e as suas atividades. Trata-se de uma publicação complementar do relatório mais pormenorizado da ENISA **«Cybersecurity for SMES – Challenges and Recommendations»**.

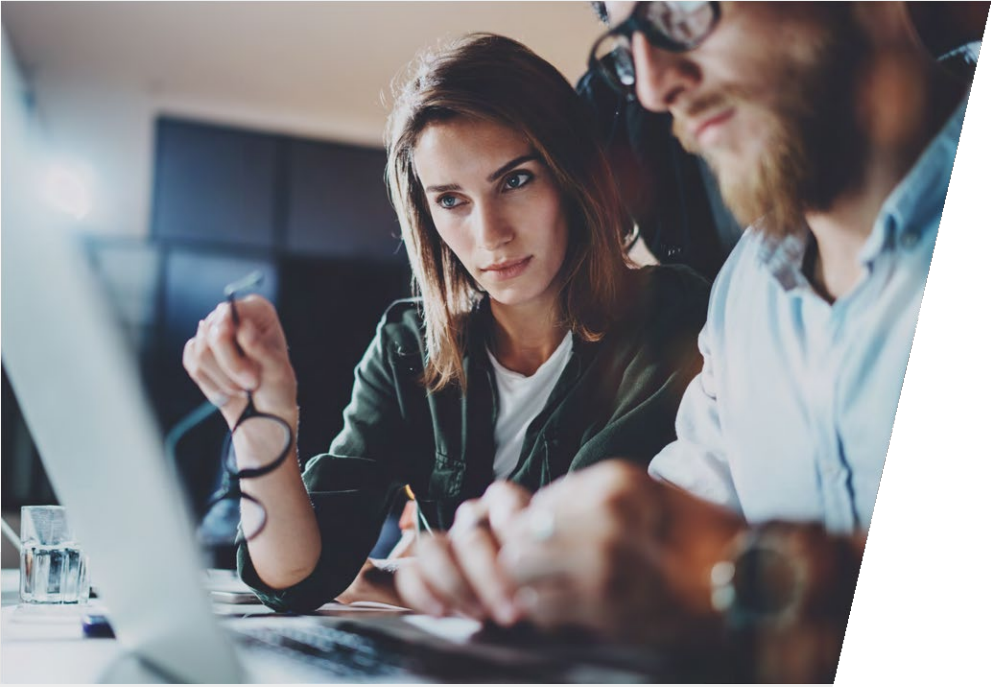
1 DESENVOLVER UMA BOA CULTURA DE CIBERSEGURANÇA

ATRIBUIR RESPONSABILIDADE DE GESTÃO

A boa cibersegurança é um elemento-chave para o sucesso contínuo de qualquer PME. A responsabilidade por esta função crítica deve ser atribuída a alguém dentro da organização que deverá assegurar recursos adequados, tais como tempo de trabalho, a aquisição de *software*, serviços e equipamento informático de cibersegurança, a formação do pessoal e o desenvolvimento de políticas eficazes para a cibersegurança.

OBTER A ACEITAÇÃO DOS FUNCIONÁRIOS

Obtenha a aceitação dos funcionários através de uma comunicação eficaz sobre cibersegurança por parte da administração, mostrando abertamente o apoio por parte da administração a iniciativas de cibersegurança, administrando aos funcionários formações adequadas e fornecendo-lhes regras claras e específicas delineadas em conformidade com políticas de cibersegurança.



PUBLICAR POLÍTICAS DE CIBERSEGURANÇA

Deverão ser definidas regras claras e específicas nas políticas de cibersegurança para os funcionários sobre a forma como se deverão comportar quando utilizarem o ambiente, o equipamento e os serviços de TIC da empresa. Estas políticas devem também destacar as consequências em caso de incumprimento. As políticas precisam de ser revistas e atualizadas regularmente.

REALIZAR AUDITORIAS DE CIBERSEGURANÇA

Devem ser realizadas auditorias regulares por pessoas com conhecimentos, aptidões e experiência adequados. Os auditores devem ser independentes, quer sejam contratantes externos ou internos das PME e independentes das operações diárias das TI.

RECORDAR A PROTEÇÃO DE DADOS

Nos termos do Regulamento Geral de Proteção de Dados da UE[1], as PME que processem ou armazenem dados pessoais pertencentes a residentes na UE/EEE devem garantir a existência de controlos de segurança adequados para proteger esses dados, incluindo assegurar que os terceiros que trabalhem em nome da PME dispõem de medidas de segurança adequadas.

1 Regulamento Geral de Proteção de Dados https://ec.europa.eu/info/law/law-topic/data-protection_pt

2

PROPORCIONAR A FORMAÇÃO ADEQUADA

Administre formações de sensibilização para a cibersegurança regulares a todos os funcionários para garantir que estes saibam reconhecer e lidar com as várias ciberameaças. Estas formações devem ser adaptadas às PME e focarem-se em situações da vida real.

Ofereça formação interna especializada em cibersegurança aos responsáveis pela gestão da cibersegurança, a fim de garantir que estes disponham das aptidões e competências necessárias para o desempenho das suas funções.

3

GARANTIR UMA GESTÃO EFICAZ DE TERCEIROS

Garanta que todos os fornecedores, especialmente aqueles com acesso a dados e/ou sistemas sensíveis, são geridos ativamente e atendem aos níveis de segurança acordados. Devem ser estabelecidos acordos contratuais para regular o modo como os fornecedores cumprem esses requisitos de segurança.

4

DESENVOLVER UM PLANO DE RESPOSTA A INCIDENTES

Elabore um plano formal de resposta a incidentes, que contenha orientações, papéis e responsabilidades claras e documentadas para garantir que todos os incidentes de segurança são respondidos de forma atempada, profissional e adequada. Para responder rapidamente a ameaças de segurança, investigue ferramentas que possam monitorizar e criar alertas quando estiverem a ocorrer atividades suspeitas ou violações de segurança.

5 PROTEGER O ACESSO AOS SISTEMAS

Encoraje todos a usar uma frase-chave, um conjunto de pelo menos três palavras comuns aleatórias combinadas numa frase que forneça uma excelente combinação entre facilidade de memorização e segurança. Se optar por uma palavra-passe típica:

- Crie uma palavra-passe longa, com letras minúsculas e maiúsculas, possivelmente também com números e caracteres especiais.
- Evite palavras-passe óbvias, tais como «palavra-passe», sequências de letras ou números como «abc» ou «123».
- Evite usar informações pessoais que possam ser encontradas em linha.

E quer utilize frases-chave ou palavras-passe:

- Não as reutilize noutro local.
- Não as partilhe com colegas.
- Ative a autenticação de dois fatores.
- Use um gestor dedicado a palavras-passe.

6

PROTEGER OS DISPOSITIVOS

Manter os dispositivos usados pelo pessoal seguros, sejam os seus computadores de secretária, computadores portáteis, computadores *tablet* ou telemóveis inteligentes, é um passo fundamental num programa de cibersegurança.

MANTER O *SOFTWARE* ATUALIZADO

De preferência, com recurso a uma plataforma centralizada para gerir as atualizações. Recomenda-se vivamente às PME que:

- Atualizem regularmente todo o*software*.
- Ativem as atualizações automáticas sempre que possível.
- Identifiquem o *software* e o equipamento informático que requer atualizações manuais.
- Tomem em consideração os dispositivos móveis e a IdC.

USAR UM ANTIVÍRUS

Deve ser implementada uma solução antivírus gerida centralmente em todos os tipos de dispositivos, que deve ser mantida atualizada para garantir a sua eficácia contínua. Além disso, não instale *software* contrafeito, pois este pode conter programas maliciosos.

USAR FERRAMENTAS DE PROTEÇÃO DE CORREIO ELETRÓNICO E DA WEB

Utilize soluções para bloquear mensagens eletrónicas não solicitadas (*spam*), com ligações para sítios Web maliciosos ou com anexos maliciosos, como, por exemplo, vírus, e *phishing*.

ENCRIPTAR OS DADOS

Proteja os dados através do uso de encriptação. As PME devem garantir que os dados armazenados em dispositivos móveis, tais como computadores portáteis, telemóveis inteligentes e computadores tablet, são encriptados. Para dados transferidos através de redes públicas, tais como redes locais sem fios de hotéis ou aeroportos, certifique-se de que os dados são encriptados, quer através do uso de uma rede privada virtual (VPN) ou acedendo a sítios Web por meio de ligações seguras usando o protocolo SSL/TLS. Certifique-se de que os seus próprios sítios Web estão a utilizar tecnologia de encriptação adequada para proteger os dados dos clientes na Internet.

7 PROTEGER A SUA REDE

IMPLEMENTAR A GESTÃO DE DISPOSITIVOS MÓVEIS

Ao facilitar o teletrabalho, muitas PME permitem que os funcionários usem os seus próprios computadores portáteis, computadores *tablet* e/ou telemóveis inteligentes. Isso introduz várias preocupações de segurança sobre dados comerciais confidenciais armazenados nesses dispositivos. Uma forma de gerir esse risco é empregar uma solução de gestão de dispositivos móveis (MDM), permitindo que as PME:

- Controlem que dispositivos podem aceder aos seus sistemas e serviços.
- Assegurem que o dispositivo tem antivírus atualizado instalado.
- Determinem se o dispositivo está encriptado.
- Confirmem se o dispositivo tem uma atualização corretiva instalada.
- Implementem a proteção do dispositivo através de um código PIN e/ou de uma palavra-passe.
- Eliminem remotamente dados da PME do dispositivo se o proprietário do dispositivo comunicar que o mesmo se perdeu ou foi roubado, ou se o contrato do proprietário do dispositivo com a PME terminar.

USAR *FIREWALLS*

As *firewalls* gerem o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas das PME. Devem ser implementadas para proteger todos os sistemas críticos, em especial para proteger a rede das PME da Internet.

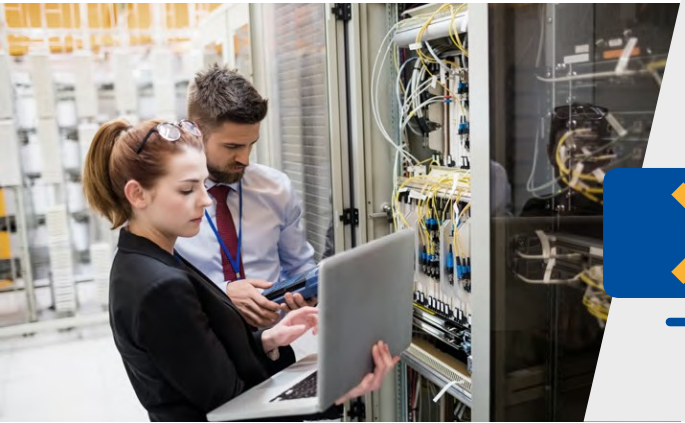
REVER SOLUÇÕES DE ACESSO REMOTO

As PME devem rever regularmente todas as ferramentas de acesso remoto para garantir a sua segurança, particularmente:

- Assegurar que todo o *software* de acesso remoto está atualizado.
- Restringir o acesso remoto de locais geográficos suspeitos ou de determinados endereços IP.
- Restringir o acesso remoto do pessoal apenas aos sistemas e computadores necessários para a execução do seu trabalho.
- Implementar palavras-passe fortes para acesso remoto e, sempre que possível, ativar a autenticação de dois fatores.
- Garantir que a monitorização e o alerta estão ativados para avisar sobre ataques suspeitos ou atividades suspeitas invulgares.

8 MELHORAR A SEGURANÇA FÍSICA

Devem ser utilizados controlos físicos adequados sempre que existam informações importantes. Um computador portátil ou um telefone inteligente da empresa, por exemplo, não deve ser deixado sem vigilância no banco traseiro de um carro. Sempre que um utilizador se afasta do computador, deve bloqueá-lo. Em alternativa, deve ativar a função de bloqueio automático em dispositivos usados para fins comerciais. Os documentos sensíveis impressos também não devem ser deixados sem vigilância e, quando não estiverem em uso, devem ser armazenados com segurança.



9 PROTEGER AS SALVAGUARDAS (*BACKUPS*)

Para permitir a recuperação de informações-chave, devem ser mantidas salvaguardas, pois são uma forma eficaz de recuperar de incidentes como um ataque de *software* de sequestro. Devem ser aplicadas as seguintes regras de salvaguarda:

- a salvaguarda é regular e automatizada sempre que possível,
- a salvaguarda é mantida separadamente do ambiente de produção das PME,
- as salvaguardas são encriptadas, especialmente se forem movidas entre locais,
- é testada regularmente a capacidade de restaurar dados a partir das salvaguardas. Idealmente, deve ser feito um teste regular de restauração total do início ao fim.

10

TRABALHAR NA NUVEM

Embora ofereça muitas vantagens, as soluções baseadas em nuvem apresentam alguns riscos únicos, os quais as PME devem considerar antes de recorrerem a um prestador de serviços de computação em nuvem. A ENISA publicou um «Cloud Security Guide for SMEs»[2], o qual as PME devem consultar quando migram para a nuvem.

Quando selecionam um prestador de serviços de computação em nuvem, as PME devem assegurar-se de que não violam leis nem regulamentos ao armazenar dados, especialmente dados pessoais, fora da UE/EEE. Por exemplo, o RGPD da UE exige que os dados pessoais de residentes da UE/EEE não sejam armazenados nem transmitidos fora da UE/EEE, exceto em condições muito específicas.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 SÍTIOS WEB EM LINHA SEGUROS

É essencial que as PME assegurem que os seus sítios Web em linha sejam configurados e mantidos de forma segura e que os dados pessoais ou informações financeiras, tais como dados de cartões de crédito, sejam protegidos adequadamente. Isso implicará a realização de testes de segurança regulares dos sítios Web, para identificar possíveis irregularidades de segurança e realizar revisões regulares para garantir que o sítio Web seja mantido e atualizado corretamente.

12 PESQUISAR E PARTILHAR INFORMAÇÕES

Um instrumento eficaz na luta contra o cibercrime é a partilha de informação. A partilha de informação relativa ao cibercrime é fundamental para que as PME compreendam melhor os riscos que enfrentam. As empresas que ouvem falar sobre os desafios da cibersegurança e sobre como esses desafios foram superados pelos pares irão, mais provavelmente, tomar medidas para proteger os seus sistemas do que se retirassem informações semelhantes de relatórios especializados ou de estudos de cibersegurança.

AGÊNCIA DA UNIÃO EUROPEIA
PARA A CIBERSEGURANÇA

ACERCA DA ENISA

A Agência da União Europeia para a Cibersegurança, ENISA, é a agência da União dedicada à obtenção de um elevado nível comum de cibersegurança na Europa. Estabelecida em 2004 e reforçada pelo Regulamento Cibersegurança da UE, a Agência da União Europeia para a Cibersegurança contribui para a ciberpolítica da UE, reforça a fiabilidade dos produtos, serviços e processos de TIC com sistemas de certificação da cibersegurança, coopera com os Estados-Membros e os organismos da UE e ajuda a Europa a preparar-se para os desafios cibernéticos do futuro. Através da partilha de conhecimentos, do reforço das capacidades e da sensibilização, a Agência trabalha em colaboração com as suas principais partes interessadas para reforçar a confiança na economia conectada, aumentar a resiliência das infraestruturas da União e, em última análise, manter a segurança digital da sociedade e dos cidadãos europeus. Para mais informações, consultar www.enisa.europa.eu.

ENISA
Agência da União Europeia para a Cibersegurança

Delegação de Atenas
Ethnikis Antistaseos 72 e
Agamemnonos 14,
Chalandri 15231, Attiki, Grécia

Delegação de Heraclião
95 Nikolaou Plastira 700 13
Vassilika Vouton, Heraclião,
Grécia

enisa.europa.eu