enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cybersecurity guide for SMEs

12 STEPS TO SECURING YOUR BUSINESS

The COVID-19 crisis showed how important the Internet and computers in general are for SMEs. In order to thrive in business during the pandemic many SMEs had to take business continuity measures, such as adopting to cloud services, improving their internet services, upgrading their websites and enabling staff to work remotely.

This leaflet provides SMEs with practical 12 high level steps on how to better secure their systems and their business. It is a companion publication to the more detailed ENISA report **"Cybersecurity for SMES – Challenges and Recommendations"**.

1 DEVELOP GOOD CYBERSECURITY CULTURE

ASSIGN MANAGEMENT RESPONSIBILITY

Good cybersecurity is a key element in the ongoing success of any SME. Responsibility for this critical function should be assigned to someone within the organization who should ensure appropriate resources such as time from personnel, the purchasing of cybersecurity software, services and hardware, training for staff, and the development of effective policies are given to cybersecurity.

GAIN EMPLOYEE BUY-IN

Gain employee buy-in through effective communication on cybersecurity from management, by management openly supporting cybersecurity initiatives, appropriate trainings delivered to employees, and providing employees with clear and specific rules outlined in cybersecurity policies.

PUBLISH CYBERSECURITY POLICIES

Clear and specific rules should be outlined in cybersecurity policies for employees on how they are expected to behave when using the company's ICT environment, equipment and services. These policies should also highlight the consequences an employee could face should they not adhere to the policies. The policies need to be regularly reviewed and updated.

CONDUCT CYBERSECURITY AUDITS

Regular audits should be carried out by those with the appropriate knowledge, skills and experience. Auditors should be independent, be it an outside contractor or internal to the SME and independent of daily IT operations.

REMEMBER DATA PROTECTION

Under the EU General Data Protection Regulation[1] any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.

1 General Data Protection Regulation https://ec.europa.eu/info/law/law-topic/data-protection_en

2

PROVIDE APPROPRIATE TRAINING

Provide regular cybersecurity awareness trainings for all employees to ensure they can recognize and deal with the various cybersecurity threats. These trainings should be tailored for SME's and focus on real-life situations.

Provide specialized cybersecurity training for those responsible for managing cybersecurity within the business to ensure they will have the skills and competencies required to do their job.

3

ENSURE EFFECTIVE THIRD PARTY MANAGEMENT

Ensure that all vendors, particularly those with access to sensitive data and/or systems, are actively managed and meet agreed levels of security. Contractual agreements should be in place to regulate how vendors meet those security requirements.

4

DEVELOP AN INCIDENT RESPONSE PLAN

Develop a formal incident response plan, which contains clear guidelines, roles and responsibilities documented to ensure that all security incidents are responded to in a timely, professional and appropriate manner. To respond quickly to security threats, investigate tools that could monitor and create alerts when suspicious activity or security breaches are occurring.

5 SECURE ACCESS TO SYSTEMS

Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security. If you opt for a typical password:

- Make it long, with lower and upper case characters, possibly also numbers and special characters.
- Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”.
- Avoid using personal info that can be found online.

And whether you use passphrases or passwords

- Do not reuse them elsewhere.
- Do not share them with colleagues.
- Enable Multi-Factor Authentication.
- Use a dedicated password manager.

6 SECURE DEVICES

Keeping the devices staff use, be their desktop PCs, laptops, tablets, or smartphones, secure is a key step in a cybersecurity program.

KEEP SOFTWARE PATCHED AND UP TO DATE

Ideally using a centralized platform to manage patching. It is highly recommended for SMEs to:

- Regularly update all of their software.
- Turn on automatic updates whenever possible.
- Identify software and hardware that requires manual updates.
- Take into account mobile and IoT devices.

ANTI-VIRUS

A centrally managed anti-virus solution should be implemented on all types of devices and kept up-to-date in order to ensure its continuous effectiveness. Also, do not install pirated software as it may contain malware.

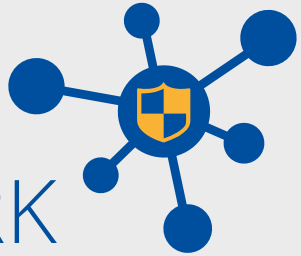
EMPLOY EMAIL AND WEB PROTECTION TOOLS

Employ solutions to block spam emails, email-containing links to malicious websites, emails containing malicious attachments such as viruses, and phishing emails.

ENCRYPTION

Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.

7 SECURE YOUR NETWORK



IMPLEMENT MOBILE DEVICE MANAGEMENT

When facilitating staff to work remotely many SMEs allow staff to use their own laptops, tablet and/or smartphones. This introduces several security concerns about sensitive business data stored on those devices. One way to manage this risk is to employ a Mobile Device Management (MDM) solution, allowing SMEs to:

- Control what devices are allowed to access its systems and services.
- Ensure the device has up to date anti-virus software installed.
- Determine if the device is encrypted.
- Confirm if the device has up to date software patches installed.
- Enforce the device is protected by a PIN and/or a password.
- Remotely wipe any SME data from the device should the device owner report it lost or stolen, or if the device owner's employment was to end with the SME.

EMPLOY FIREWALLS

Firewalls manage the traffic that enters and leaves a network and are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particular a firewall should be employed to protect the SME's network from the Internet.

REVIEW REMOTE ACCESS SOLUTIONS

SMEs should regularly review any remote access tools to ensure they are secure, particularly:

- Ensure all remote access software is patched and up date.
- Restrict remote access from suspicious geographical locations or certain IP addresses.
- Restrict staff remote access only to the systems and computers they need for their work.
- Enforce strong passwords for remote access and where possible enable multi-factor authentication.
- Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.

8 IMPROVE PHYSICAL SECURITY

Appropriate physical controls should be employed wherever important information resides. A company laptop or a smartphone, for instance, should not be left unattended in the back seat of a car. Anytime a user walks away from their computer they should lock it. Otherwise, enable auto-lock function on any device used for business purposes. Sensitive printed documents should also not be left unattended and when not in use, securely stored away.

9 SECURE BACKUPS

To enable the recovery of key formation, backups should be maintained as they are an effective way to recover from disasters such as a ransomware attack. The following backup rules should apply:

- backup is regular and automated whenever possible,
- backup is held separately from the SME's production environment,
- backups are encrypted, especially if they are going to be moved between locations,
- the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done.

10

ENGAGE WITH THE CLOUD

While offering many advantages, cloud based solutions do present some unique risks, which SMEs should consider before engaging with a cloud provider. ENISA have published a "Cloud Security Guide for SMEs"[2] which SMEs should refer to when migrating to the cloud.

When selecting a cloud provider, SME should ensure it does not breach any laws or regulations by storing data, especially personal data, outside of the EU/EEA. For example, the EU GDPR requires that personal data of residents within the EU/EEA is not stored or transmitted outside of the EU/EEA unless under very specific conditions.

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

11 SECURE ONLINE SITES

It is essential that SMEs ensure that their online websites are configured and maintained in a secure manner and that any personal data or financial details, such as credit card data, is appropriately protected. This will entail running regular security tests against the websites to identify any potential security weaknesses and conducting regular reviews to ensure the site is maintained and updated properly.

12 SEEK AND SHARE INFORMATION

An effective tool in the fight against cybercrime is the sharing of information. The sharing of information in relation to cybercrime is key to SMEs to better understand the risks they face. Firms that hear about cybersecurity challenges, and how those challenges were overcome, from their peers will more likely take steps to secure their systems than if they were to hear similar details from industry reports or from cybersecurity surveys.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Greece

enisa.europa.eu