23 Ιανουαρίου 2025

Κυβερνοασφάλεια για τις μικρομεσαίες επιχειρήσεις

Το Enterprise Europe Network (EEN) βρίσκεται δίπλα στις μικρές και μεσαίες επιχειρήσεις (ΜΜΕ), υποστηρίζοντάς τις στην προστασία από τις προκλήσεις του ψηφιακού κόσμου. Στόχος μας είναι να παρέχουμε στις επιχειρήσεις τα εργαλεία, τη γνώση και την καθοδήγηση που χρειάζονται για να προστατεύσουν τα ψηφιακά τους δεδομένα και τη λειτουργία τους.

Στο πλαίσιο αυτό, θα θέλαμε να σας ενημερώσουμε ότι το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) έχει αναπτύξει εκπαιδευτικό υλικό που απευθύνεται στις επιχειρήσεις, το οποίο περιγράφει τα βασικά βήματα για την εξασφάλιση ενός ασφαλούς περιβάλλοντος στον κυβερνοχώρο.

Γιατί είναι σημαντική η κυβερνοασφάλεια; Η κυβερνοασφάλεια είναι απαραίτητη εάν θέλετε να αποτρέψετε ηλεκτρονικές επιθέσεις στην επιχείρηση σας από εγκληματίες, όπως χάκερς, δεδομένου ότι οι μικρομεσαίες επιχειρήσεις τείνουν να αποτελούν τον κύριο στόχο αυτών των εγκληματιών λόγω των μικρότερων προϋπολογισμών ασφαλείας τους..

Η εξασφάλιση ενός ασφαλούς κυβερνοχώρου έχει ορισμένα βασικά πλεονεκτήματα για επιχειρήσεις:

1. Αποτρέπει οικονομικές απώλειες
2. Προστατεύει τα δεδομένα των πελατών
3. Διατηρεί το κύρος της εταιρείας

Κάποιες βασικές ενέργειες που μπορείτε να λάβετε για την βελτίωση της κυβερνοασφάλειας στην επιχείρησή σας είναι:

- **Συχνές** αξιολογήσεις ρίσκου από:
  - Προσδιορισμός βασικών περιουσιακών στοιχειών(σημαντικών δεδομένων και συστημάτων), αξιολόγηση κινδύνων, και
  - Προτεραιοποίηση ζητημάτων με υψηλό αντίκτυπο και επιδιόρθωση των αδυναμιών..
- Εκπαίδευση προσωπικού
  - **Εκπαίδευσή** για την **αναγνώριση** phishing και άλλων μορφών εξαπάτησης .
  - **Προώθηση** χρήσης ισχυρών κωδικών πρόσβασης και ασφαλούς διαδικτυακής περιήγησης.
- Έλεγχος πρόσβασης
  - Χρήση **ισχυρών, μοναδικών κωδικών πρόσβασης** για κάθε λογαριασμό και ενθάρρυνση χρήσης εργαλείων όπως password managers.
  - Ενεργοποίηση του **ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA)** για ένα επιπλέον επίπεδο ασφάλειας.
  - Παροχή πρόσβασης σε υπαλλήλους μόνο στα **απαραίτητα δεδομένα και συστήματα**.
- Ενημερώσεις λογισμικού
  - **Συνεχείς** ενημέρωση συστημάτων με τις τελευταίες επιδιορθώσεις ασφαλείας.
  - **Αποφυγή** χρήσης **ξεπερασμένου ή μη υποστηριζόμενου** λογισμικού.
- Προστασία δεδομένων και δημιουργία αντιγράφων ασφαλείας (back-up)
  - **Κρυπτογράφηση** ευαίσθητων δεδομένων και ασφαλής αποθήκευση.

- Δημιουργία **αντιγράφων ασφαλείας(back-up)** των δεδομένων σε τακτά χρονικά διαστήματα και αποθήκευση των αντιγράφων ασφαλείας σε ασφαλή τοποθεσία.

- Ασφάλεια δικτύου
  - Ρύθμιση **firewalls** για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.
  - **Ασφάλιση** Wi-Fi με την χρήση ισχυρών κωδικών πρόσβασης και ενεργοποίηση κρυπτογράφησης.
- Σχέδιο αντιμετώπισης περιστατικών
  - Δημιουργία **σχεδίου αντίδρασης** για πιθανές επιθέσεις στον κυβερνοχώρο.
  - Δοκιμή του σχεδίου για να διασφαλιστεί ότι όλοι γνωρίζουν τι πρέπει να κάνουν σε περίπτωση συμβάντος.
- Εξειδικευμένη υποστήριξη
  - Συνεργασία με **ειδικούς ή εμπειρογνώμονες** σε θέματα κυβερνοασφάλειας ή χρήση υπηρεσιών διαχειριζόμενης ασφάλειας για πρόσθετη προστασία.
- **Διασφάλιση της συμμόρφωσης** με τους νόμους περί προστασίας δεδομένων και τα πρότυπα του κλάδου για την αποφυγή νομικών ζητημάτων.

Για πιο εμπεριστατωμένη καθοδήγηση μπορείτε να διαβάστε τον πλήρη οδηγό που ακολουθεί ποιο κάτω. Είναι διαθέσιμος στα αγγλικά και διαβάζετε μέσα σε μόνο 5 λεπτά!

Εκτός από τον συγκεκριμένο οδηγό, υπάρχει διαθέσιμο και επιπλέον εκπαιδευτικό υλικό που μπορεί να σας φανεί χρήσιμο. Για να δείτε όλους τους οδηγούς και να αποκτήσετε περισσότερες πληροφορίες, επισκεφθείτε την ενότητα εκπαιδευτικού υλικού στην επίσημη ιστοσελίδα του NCC-CY.

Παραμένοντας στη διάθεσή σας.
Με εκτίμηση,

Χριστίνα Παναγίδη
Λειτουργός ΚΕΒΕ
Τμήμα Ευρωπαϊκών Θεμάτων και Προγραμμάτων
Σύμβουλος Enterprise Europe Network Κύπρου
Τηλ. 22889766, c.panayides@ccci.org.cy
https://een.ec.europa.eu

23 January 2025

Cybersecurity for Small and Medium Enterprises (SMEs)

The **Enterprise Europe Network (EEN) Cyprus** is committed to supporting small and medium-sized enterprises (SMEs), encouraging their protection from the challenges of the cyber world. Our goal is to provide the tools, knowledge and guidance needed for small and medium enterprises (SMEs) for them to protect their databases and operation.

In this regard, we would like to inform you that the Cybersecurity National Coordination Centre (NCC) has developed education material on cybersecurity tailored to SMEs, outlining the key steps to ensure a safe and secure cyber environment.

Why is Cybersecurity important for smaller enterprises? Cybersecurity is essential if you want to prevent cyber-attacks from cybercriminals, like hackers for example, since SMEs tend to be the main target for such criminals due to their smaller security budgets.

Ensuring a secure cyberspace has some key advantages for businesses:

1. Prevents financial losses
2. Protects customer data
3. Maintains company reputation

Some basic steps to take to improve the cybersecurity of your enterprise are:

- Performing **regular** risk assessments by
  - Identifying key assets (important data and systems) and assessing risks, and
  - Fixing vulnerabilities by prioritizing high-impact issues.
- Employee Training
  - **Teaching** staff to **recognize** phishing emails and other scams.
  - **Promoting** strong password habits and safe browsing practices.
- Access Control
  - Using **strong, unique passwords** for **each account** and encouraging password managers.
  - **Enabling Multi-Factor Authentication** (MFA) for an extra layer of security.
  - Giving employees access only to necessary systems and data.
- Software Updates
  - Keeping systems **up to date** with the latest security patches.
  - **Avoiding** the use of **outdated** or unsupported software.
- Data Protection & Backup
  - **Encrypting sensitive data** and storing it securely.
  - Backing up data regularly and **storing backups in a secure location**.
- Network Security
  - Installing and configuring **firewalls** to block unauthorized access.
  - Securing your Wi-Fi with strong passwords and encryption.
- Incident Response Plan
  - **Preparing** for potential cyberattacks with a **clear plan** on how to respond.
  - **Testing the plan** to ensure everyone knows what to do in case of an incident.

- Expert Support
    - If needed, hire a **cybersecurity expert** or use **managed security services** for added protection.
- **Ensuring compliance** with data protection laws and industry standards to avoid legal issues.

For more in-depth guidance please read the full guide below. Reading the guide will take approximately 5 minutes.

For more guides and training materials on cybersecurity please visit the educational material section found on the NCC-CY official site.

Remaining at your disposal.
Yours faithfully,

Christina Panayides
Officer CCCI
Department of European Affairs & Programmes
Advisor of Enterprise Europe Network Cyprus
Tel. 22889766, c.panayides@ccci.org.cy
https://een.ec.europa.eu

TLP: WHITE

Cybersecurity for SMEs

Guide

NCC CYBERSECURITY NATIONAL COORDINATION CENTRE CYPRUS

COMMISSIONER OF COMMUNICATIONS Digital Security Authority

Co-funded by the European Union

ncc.cy

Contents

01

Introduction

Importance of Cybersecurity for SMEs

Cybersecurity is crucial for small and medium-sized enterprises (SMEs) as they are increasingly targeted by cybercriminals. Protecting your business from cyber threats can prevent financial loss, protect customer data, and maintain your business's reputation.

Overview of the Cybersecurity Landscape in Cyprus

Cyprus, like many other regions, faces a growing number of cyber threats. SMEs are particularly vulnerable due to limited resources and awareness. Understanding these threats and taking proactive measures is essential for safeguarding your business.

Cybersecurity Fundamentals

02

Basic Concepts of Cybersecurity

Cybersecurity involves protecting systems, networks, and data from digital attacks. Key concepts include:

- Confidentiality: Ensuring that information is accessible only to those authorized to have access.
- Integrity: Protecting data from being altered or destroyed in an unauthorized manner.
- Availability: Ensuring that data and services are available to authorized users when needed.

Common Types of Cyber Threats

Cybersecurity involves protecting systems, networks, and data from digital attacks. Key concepts include:

- Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems.
- Ransomware: A type of malware that encrypts a victim's files and demands a ransom for the decryption key.
- Phishing: Deceptive attempts to obtain sensitive information by disguising as a trustworthy entity.

03

Cybersecurity Measures for SMEs

Network Security

Firewalls

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between your internal network and external sources, filtering traffic to prevent unauthorized access.

Data Protection

Data Encryption

Encrypt sensitive data to protect it from unauthorized access.

Action Steps:

- Use encryption tools to encrypt data at rest and in transit.
- Regularly update encryption keys.
- Train employees on the importance of data encryption.

Data Protection

Secure Data Backup

Regularly back up data and store backups securely to prevent data loss.

Action Steps:

- Implement an automated backup solution.
- Store backups in a secure, offsite location.
- Regularly test backups to ensure data can be restored.

Access Control

Password Policies

Strong passwords are essential for protecting accounts and systems.

Action Steps:

- Enforce the use of complex passwords (at least 12 characters, including letters, numbers, and special characters).
- Implement regular password changes.
- Educate employees on the importance of using unique passwords for different accounts.

Access Control

Multi-Factor Authentication

Add an extra layer of security by requiring multiple forms of verification.

Action Steps:

- Implement multi-factor authentication (MFA) for all critical systems.
- Use MFA for remote access and sensitive applications.
- Regularly review and update MFA settings.

Incident Response

Steps to Take During a Cyber Incident

Having a plan in place for responding to cyber incidents can minimize damage.

Action Steps:

- Identify and contain the incident.
- Notify relevant stakeholders.
- Eradicate the cause of the incident and recover affected systems.
- Conduct a post-incident review to identify lessons learned.

Incident Response Planning

Develop a comprehensive incident response plan to ensure preparedness.

Action Steps:

- Define roles and responsibilities for incident response.
- Develop procedures for detecting, responding to, and recovering from incidents.
- Regularly test and update the incident response plan.

Overview of Relevant Regulations (e.g., GDPR)

Understand and comply with legal requirements related to data protection and privacy.

Best Practices for SMEs

04

Employee Training

Cybersecurity Awareness Programs

Educate employees on cybersecurity risks and best practices.
Action Steps:

- Conduct regular cybersecurity awareness training.
- Provide resources and materials on common threats.
- Encourage a culture of security awareness.

Employee Training

Phishing Simulations

Test and improve employees' ability to recognize phishing attempts.
Action Steps:

- Conduct regular phishing simulations.
- Provide feedback and additional training based on simulation results.
- Reward employees who demonstrate strong security awareness.

Regular Updates and Patch Management

Importance of Keeping Software and Systems Updated.

Regularly update software and systems to protect against vulnerabilities.

Action Steps:

- Enable automatic updates for operating systems and applications.
- Regularly review and apply security patches.
- Maintain an inventory of software and hardware to track updates.

Secure Remote Work Practices

VPNs

Use virtual private networks (VPNs) to secure remote connections.

Action Steps:

- Implement a VPN solution for remote employees.
- Require employees to use the VPN for accessing company resources.
- Regularly update and monitor the VPN solution.

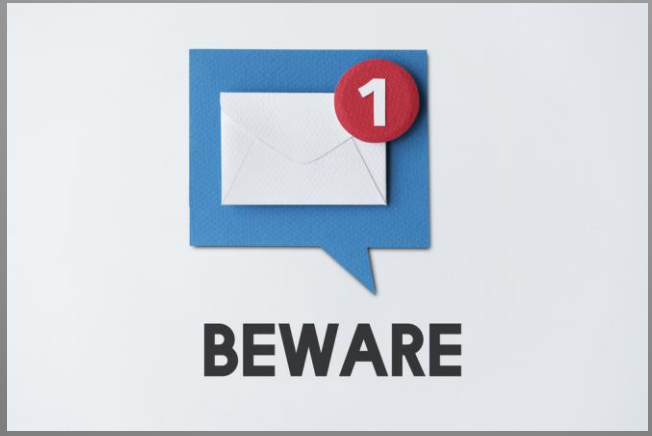
Secure Remote Work Practices

Secure Communication Tools

Implement secure tools for remote communication and collaboration.

Action Steps:

- Use encrypted communication tools (e.g., secure email, messaging apps).
- Train employees on the use of secure communication tools.
- Regularly review and update communication security policies.



Vendor and Third-Party Risk Management

Assessing Third-Party Security

Evaluate the cybersecurity practices of vendors and partners.

Action Steps:

- Conduct security assessments of third-party vendors.
- Include cybersecurity requirements in vendor contracts.
- Regularly review and update vendor security practices.

Vendor and Third-Party Risk Management

Contracts and SLAs

Include cybersecurity requirements in contracts and service level agreements.

Action Steps:

- Define security expectations and responsibilities in contracts.
- Monitor compliance with contractual security requirements.
- Review and update contracts and SLAs regularly.

05

Resources and tools

Cybersecurity resources for basic protection

- Antivirus Software
- Firewalls
- Encryption Tools
- Backup Solutions

Government and Local Resources

- Cyprus Police Cybercrime Department: Provides support and resources for cybercrime incidents.
- Cyprus Computer Emergency Response Team (CY-CERT): Offers guidance and incident response services.

Case Studies and Examples

06

Real-Life Examples of Cyber Incidents Affecting SMEs in Cyprus

Case Study 1: A local SME fell victim to a ransomware attack, resulting in the encryption of critical business data. The company had to pay a significant ransom to regain access to their data. This incident could have been prevented with regular data backups and employee training on recognizing phishing emails.

Case Study 2: Another SME experienced a data breach due to weak password practices. Cybercriminals accessed the company's network using a compromised employee account with a weak password. Implementing strong password policies and multi-factor authentication could have prevented this breach.

Lessons Learned and Prevention Tips

- Regularly Back Up Data: Ensure that data is backed up regularly and stored securely.
- Employee Training: Conduct regular training sessions on recognizing cyber threats and following best practices.
- Strong Password Policies: Enforce the use of strong, unique passwords and implement multi-factor authentication.
- Incident Response Planning: Develop and regularly test an incident response plan to ensure preparedness.

07

Cyber-Hygiene

The Cyber-Hygiene Framework

- Security Policy
  The organisation's senior management has created, approved and communicated its cybersecurity policy internally and externally. The cybersecurity policy shall be reviewed at least once a year and updated as required.

- Awareness and training
  Staff employed by the organisation and users who have access to its information (regardless of their employment relationship) must be aware of information security and in particular how they contribute to it through their role. Appropriate cybersecurity awareness activities shall be carried out on a regular basis and at least once a year.

The Cyber-Hygiene Framework

- Software Update
  The organisation's IT and communications systems must have the latest security updates installed provided only from trusted sources (e.g. the manufacturer).

- Protection from Malicious software
  Malicious software protection programmes and functions are installed throughout the organisation's IT and communication systems. Updates are made on a regular basis.

The Cyber-Hygiene Framework

- Network Security
  The organisation has installed and configured firewalls at appropriate points in its network, in order to effectively protect its systems and information from relevant threats.

- Backups
  The organisation identifies its critical information and backs up its critical information on a regular basis in accordance with the relevant backup policy.

- Access Control
  The organisation shall identify the places where important information is located. For the information and based on the type, the use and the criticality, the organisation has created a structure in an appropriate storage area, which allows it to grant access rights to authorised and authenticated users following the need-to-know principle.

The Cyber-Hygiene Framework

- Security Incidents
  The organisation has established a structure and process for responding to security incidents. The staff involved in the respective procedures are appropriately trained.

- Physical Security Measures
  The organisation has adopted physical security measures to protect the systems and facilities from any natural and environmental threats.

- Data Protection
  The organisation shall design, implement, adopt and publish a Personal Data Protection Policy based on the general GDPR regulation.

The Cyber-Hygiene Framework

- Operational Impact Analysis
  The organisation has designed and implemented an appropriate methodology for operational impact analysis. The results and key metrics resulting from the application of the methodology are recorded, maintained and feed into the design of relevant measures and implementations.

08

Conclusion

Recap of the Importance of Cybersecurity

Cybersecurity is critical for protecting your business from financial loss, data breaches, and reputational damage. By implementing the measures outlined in this guide, SMEs in Cyprus can significantly enhance their cybersecurity posture.

Encouragement to Implement The Cyber-Hygiene Framework

Take proactive steps to safeguard your business by following the recommendations in this guide. Regularly review and update your cybersecurity practices to stay ahead of emerging threats. Remember, cybersecurity is an ongoing process that requires vigilance and continuous improvement.

National Grant to enhance Cybersecurity in SME's by NCC-CY

The National Cyber Security Coordination Centre of the Republic of Cyprus was established with the adoption of the European Regulation (EU) 2021/887 and has undertaken to play an important role for Cyprus and the Union. Within the framework of the Regulation, the Centre undertakes actions at national level and internationally, through partnerships and joint actions, aiming at providing economic support to various stakeholders.

That is provision of support to Small and Medium Enterprises - SMEs, to improve their level of security and resilience, to enhance research and innovation, support for technological and industrial development, as well as to build cybersecurity capacity and skills.

Visit the NCC-CY website for more information regarding the National Grant and further to explore future events

References:

1.Advanced Persistent Threats (APTs)

1. FireEye. (2019). "APT28: A Window into Russia's Cyber Espionage Operations?" [Online]. Available: https://www.fireeye.com/current-threats/apt-groups.html
2. CrowdStrike. (2021). "CrowdStrike Global Threat Report." [Online]. Available: https://www.crowdstrike.com/resources/reports/global-threat-report/

2.Cyber Espionage

1. Symantec. (2016). "Operation Shady RAT." [Online]. Available: https://www.symantec.com/connect/blogs/operation-shady-rat-revealed
2. Mandiant. (2013). "APT1: Exposing One of China's Cyber Espionage Units." [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

3.Disruptive and Destructive Attacks

1. Zetter, K. (2014). "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon." Crown.
2. Wired. (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

References:

1.Supply Chain Attacks

1. SolarWinds. (2021). "What You Need to Know About the SUNBURST / SolarWinds Orion Supply Chain Attack." [Online]. Available: https://www.solarwinds.com/securityadvisory
2. Cisco Talos. (2017). "CCleaner Supply Chain Attack." [Online]. Available: https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

2.Critical Infrastructure Attacks

1. Dragos. (2017). "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations." [Online]. Available: https://www.dragos.com/resource/crashoverride/
2. Schneider Electric. (2018). "Triton/Trisis Malware: A New Dimension of Threats." [Online]. Available: https://www.schneider-electric.com/en/download/document/998-20493509_GMA-US/

3.Data Breaches

1. Equifax. (2019). "Equifax Cybersecurity Incident & Important Consumer Information." [Online]. Available: https://www.equifaxsecurity2017.com/
2. Yahoo. (2016). "An Important Message About Yahoo User Security." [Online]. Available: https://help.yahoo.com/kb/SLN27925.html

References:

1.Phishing and Social Engineering

1. Verizon. (2021). "2021 Data Breach Investigations Report." [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/
2. KnowBe4. (2021). "Phishing and Social Engineering: Understanding the Risks." [Online]. Available: https://www.knowbe4.com/whitepaper-phishing-and-social-engineering

2.Influence and Disinformation Campaigns

1. U.S. Senate Select Committee on Intelligence. (2019). "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election." [Online]. Available: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
2. FireEye. (2020). "Ghostwriter Influence Campaign: An Overview." [Online]. Available: https://www.fireeye.com/blog/threat-research/2020/08/ghostwriter-influence-campaign.html

3.Ransomware

1. Europol. (2017). "WannaCry Ransomware Attack." [Online]. Available: https://www.europol.europa.eu/newsroom/news/global-impact-of-wannacry-ransomware-attack
2. U.S. Department of Justice. (2021). "JBS Pays $11 Million in Ransom After Cyberattack." [Online]. Available: https://www.justice.gov/opa/pr/jbs-pays-11-million-ransom-after-cyberattack