Cybersecurity awareness

This is one of the quick win strategies in the COM^3 quick win strategy series. Find all available quick win strategies at www.ruraldigital.eu.

THE RISE OF CYBERATTACKS

The increase in the number of att acks across diverse digital infrastructures calls for a need for cybersecurity awareness. Adversaries continue to target enterprises regardless of their size. It is imperative to raise awareness to limit the attack surface. The exponential growth in digitalization and the demand for context-aware processing have led to a rise in Internet-connected services, thereby increasing the risk of cyber attacks. Recent observations on the prevailing strategy of cyberattacks suggest the significance and high impact. The strategies employed by threat actors have matured to be more discrete, audacious, and impactful, targeting any form of digital entities ranging from human wearable devices to low earth orbit satellites.

THREAT FOR SMES

In light of the high demand for contextual data and accessibility, security has assumed minor importance. Over the years, the digital ecosystem has been targeted by cyber adversaries for fun and profit. With the development of digital systems and networks, the complexity and discreetness of attacks further reformed. Advancing defensive security strategies and awareness is imperative to address and limit the impact of cyberattacks. This is different for small and medium-sized enterprises (SMEs), where a recent Danish analysis demonstrates that 40% of the companies have a digital security level that needs to be higher compared to their risk profile. It is hence necessary to create awareness and emphasize the need for cybersecurity measures in SMEs.

CYBERSECURITY AWARENESS

Cybersecurity awareness is an ongoing process of educating and training employees and individuals about the threats in cyberspace and how to prevent such threats to reduce the overall cyber risk and impact. This document highlights three quick-win strategies under the cybersecurity awareness process to identify cyber threats to organizations through self-assessments. The strategies for quick wins are delivered in the form of interactive and educative online courses that help organizations improve their cybersecurity posture.

Partner meeting in Vejle
Visit Vejle – Vinter/Spring 2023
vejle
Interreg North Sea Region
What do you like to see?
And most important deep dive into?
DigitalLead
com³

@dalapeter_photography

KEY MESSAGE

- There is an increase in cyberattacks in diverse sectors, and it is imperative to have security awareness to limit the attack surface. Adversaries constantly improve their attack strategies and do not discriminate the targets based on size.
- Cybersecurity awareness can help fill the knowledge gaps essential to a secure environment and ensure minimal cyberattack impact.
- The training materials from the COM^3 project aim at providing cybersecurity awareness to SMEs as quick-win strategies. Stay secure, stay safe!

THE STRATEGIES

Aalborg University provides **three online courses** as quick win strategies for SMEs to enhance their security posture and get an overview of the attack landscape. One of the key strategies to identify active cyber threats to an organization is to use deception-based systems. Deception Systems are a strategy in Defensive Security where the systems emulate the vulnerable services of a real system to attract attackers while trapping them. The use of deception to lure attackers dates back centuries when kings used deceptive strategies to identify spies in their kingdoms. The systems mimic the behavior of the real systems to lure the attackers and exploit them. The course "Cybersecurity Readiness through Honeypots" provides an overview of how organizations can leverage Honeypots, a deception-based security system, to identify attacks and proactively plan for defenses against them.

Identifying cyber threats through Deception-based systems

One of the key strategies to identify active cyber threats to an organization is to use deception-based systems. Deception Systems are a strategy in Defensive Security where the systems emulate the vulnerable services of a real system to attract attackers while trapping them. The use of deception to lure attackers dates back centuries when kings used deceptive strategies to identify spies in their kingdoms. The systems mimic the behavior of the real systems to lure the attackers and exploit them. The course "Cybersecurity Readiness through Honeypots" provides an overview of how organizations can leverage Honeypots, a deception-based security system, to identify attacks and proactively plan for defenses against them.

Data Breach and Privacy Leak awareness

In today's digital era, data is considered a valued asset. Companies and organizations affected by data leaks incur up to $ 150 million yearly in compensation worldwide. Moreover, adversaries need to leverage better practices and gaps in digital infrastructure to plan their exploits. This course provides insight into the impact of data leaks and the risks of having a privacy leak. This course also provides an understanding of data leaks and how to identify or mitigate them.

Threat Reduction and Self-assessment for SMEs

Cyber attacks are becoming an increasing risk to digital enterprises. Adversaries are evolving their strategies for attacks to cause significant impacts. This course introduces techniques for threat reduction and self-assessment for SMEs. With this course, SMEs can use tools and methods to identify potential risks in their digital infrastructure.

RECOMMENDATIONS

- The European Union Agency for Cybersecurity (ENISA) lists the cybersecurity challenges and provides suggestions for European SMEs as a report. In addition, the report provides proposals for actions that Member States should consider to support SMEs in improving their cybersecurity posture.

- ENISA further provides a 12-step guide to securing digitalized businesses. This short guide gives SMEs 12 practical high-level steps to better secure their systems and business.The report can be accessed here.

THE COM^3 PROJECT

Digitally enabled and transformed SMEs make rural areas more attractive places to live, work and invest in. Local and regional authorities need the right tools and competencies for supporting rural enterprises in their digital transformation.
COM^3 partners develop a unique support model that strengthens and empowers local and regional actors in their role as innovation facilitators and enablers.

AALBORG UNIVERSITY

This quick win strategy was written by Aalborg University (AAU) is located in Denmark in Scandinavia. As a student at AAU you acquire knowledge and competences by way of AAU's unique study method "The Aalborg Model for Problem Based Learning (PBL)". Aalborg Univeristy offers bachelor's degree programmes, master's degree programmes and exchange programmes.

FIND OUT MORE!

Scan the code to visit our website ruraldigital.eu

Interreg North Sea Region COM^3 European Regional Development Fund EUROPEAN UNION