Modern Workplace Security Assessment

SecWise

Benefits

- ✓ Understand the current cyber security threat landscape
- ✓ Gain visibility into your security posture with an assessment on your current risks and threat exposure.
- ✓ Executed by certified Cyber Security Architects
- ✓ An actionable roadmap, tailored to your business and priorities.
- ✓ Trusted Advisor/Partner (no sales pitch)

SecWise NV

Securing your Digital Transformation

Gaston Geenslaan 11, B4
3000 Leuven
www.secwise.be

A 5-day assessment to help enhance the cyber security maturity level of your organization using a 'fit-gap' analysis approach on your current cyber security defenses and with a focus on your cloud threat exposure.

In the early days of Internet, attacks were made frequently by individuals using scripts or programs to attack computer networks and websites. These were quickly replaced by multimillion-dollar criminal organizations running sophisticated playbooks and focused on monetizing attacks.

Since 2012, we have seen a big shift where nation states, and even terrorist groups, have started to get involved in cyberattacks against the private sector. These attacks include high levels of sophistication. Attacks become focused on damage and disruption, first attacking the perimeters which are least protected. This puts the modern workplace and cloud run apps in the attackers' spotlight. Fact is, that these days employees are more mobile than ever. During their travel they want to be online to be able to collaborate in real-time with others. They try to optimize workflows through all kind of mobile apps and Cloud services to get more efficient. Moreover, the border between work and private is not always clear.

The modern digital workplace makes protecting your data, identities and devices a real challenge. The introduction of this new digital estate offers a very broad attack surface for attackers. Think about the new introduced threats with BYOD, new cloud services every day, growing Shadow IT, your data and users moving constantly outside the perimeter of your organization, doing both private and professional matters. Moreover, recent breaches clearly demonstrate the traditional network security approach doesn't work anymore with the ever-changing threat landscape.

Besides attacker's threats, you also need to secure your sensitive information against unsafe use and for compliance regulations (e.g. GDPR).

What's your security posture?

We are truly in a new era where securing your network will not be sufficient anymore, even to protect that same network in the first place! We have identified that many IT security tools are not prepared to deal with these new cloud facing threats. Incident detection and forensics often occur too late—after the breach—and it can take months before one notices they have been compromised.

Addressing attacker's threats requires an innovative approach

KNOW THE ATTACKER'S ECONOMIC MODEL + **BREAK THE ATTACK PLAYBOOK** + **FUTURE-PROOF CYBER DEFENSE DESIGN**

What can you do?

SecWise offers a Cyber Security Risk Assessment that helps you understand the current cyber security threat landscape and maps this to you current cyber security defenses. This assessment will help you plan for the future through a 'fit-gap' analysis of your '**AS IS**' defense versus **a future proof 'TO BE'** cyber security defense.

Objective of the assessment

- Overview of the current cyber security threat landscape
- FIT-GAP analysis on your current 'AS IS' cyber defense versus security gaps & risks (SANS Top 20 best-practices)
- Recommendations and 'TO BE' cyber security architecture design based on the Microsoft Security eco-system (M365 E3/E5)
- Personalized roadmap proposal based on risk prioritization

Cyber Security Risk Assesment Offer

- ✓ 5 Man-days
- ✓ Senior Cyber Security Architect
- ✓ 5.400 € in total (excL.VAT)
- ✓ Output: Fit-gap analysis, with TO BE recommendations & cyber security design
- ✓ High-level roadmap based on Risk priority

Technologies covered: *Windows 10 Secure Boot, Windows Defender (including Application control, App Guard, Credentials Guard), Windows Hello, Microsoft Defender ATP, Azure ATP, Office365 ATP, Cloud-App Security, Azure Active Directory (including Identity protection, Conditional Access, …), Azure Information Protection, Windows Information Protection, Intune Security management, O365 Security (DLP, Labels, eDiscovery, anti-phishing, Advanced Threat Protection, …)*

Note: All services will be executed in a Time & Material set-up

Take your first steps towards a more secure future! Contact us: cloudsecurity@secwise.be