WRITTEN BY

JAKUB JEDINÁK
Cybersecurity Consultant
PwC Slovakia

BUILDING A PROACTIVE CYBERSECURITY CULTURE

Most businesses concentrate on prevention and detection as their key cybersecurity strategies. On average, a breach or other type of incident, happens 212 days before initial detection[1]. Previously a reactive approach to business security was sufficient. Today, companies need to take a far more proactive approach to security.

Most companies assume they are secure, but this is an incorrect assumption. Just like with our own health, we cannot just wait for it to get to the stage when we need hospitalization. Rather, we go to the doctor regularly, we take medicine and vitamins, we take proactive measures to look after our health. The same applies to businesses' "health". Companies are often not proactive and wait for a breach to happen. They get "cybersecurity hospitalized", and then it is much harder for defense to be effective and negative impacts are often unavoidable. If we shift the mindset to "we are not secure" then we can take modern, proactive approaches to strengthen our cybersecurity.

Cybersecurity is a business issue, not just an IT problem. More security related technology isn't the solution, as human analysis and response is still required. Without trained personnel, additional security technology only generates unmanageable alerts. Businesses often have many tools and data, but lack the talent to manage them, resulting in information being overlooked. They also lack professional consulting, preventing them from seeing the "bigger picture" that unbiased expertise provides. Recognizing these issues allows for proactive cybersecurity measures.

DEFINE CYBERSECURITY POSTURE

Bulletproof security doesn't exist. With each newly added service, system or process, security decreases. There will always be threats. That's why it's crucial for companies to define what risks are acceptable and what are not, and to define their critical business assets that must be prioritized. Without a defined cybersecurity approach, every risk is accepted. It leaves a company vulnerable to unexpected breaches and incidents. A lack of preparedness can lead to significant downtime or data loss when a breach occurs. Furthermore, the cost of responding to such incidents after the fact can be far greater than the cost of guided proactive prevention.

On the other hand, no cybersecurity strategy is 100% perfect. Having defined risk approaches and strategies in place, and actively seeking to identify and mitigate potential risks before they can cause harm, reduces the likelihood of successful breaches and minimizes the impact of incidents that do occur. By investing in cybersecurity measures upfront, businesses can save a significant amount of resources in the long run.

But this is easier said than done. Frameworks and audits supported by expert guidance can help point out these risks. There are a number of applicable frameworks (e.g. NIS2, ISO, NIST, etc.) and with correct selection, thorough execution and periodical reviews, business entities can greatly boost their proactiveness as regards cybersecurity readiness.

CYBERSECURITY AWARENESS

A major cause of security breaches (more than 90%) is human error[2]. This finding supports the re-emphasized statement that cybersecurity is a business problem. Cybercriminals often exploit human nature using social engineering. Given emerging AI and the extensive availability of Ransomware-as-a-Service executed via phishing emails, businesses need to take a proactive approach by conducting high quality awareness training.

Such training needs to be tailored to business-specific needs and context. In my experience, training is often neglected, but with the use of interactive gamification, it can be very effective. Anti-phishing campaigns have also proved to be exceptionally useful, and companies state awareness training reduces phishing occurrences[3]. Last but not least, modern training simulations such as TableTop and CyberRange exercises are highly successful in building strong resilience towards social engineering.

THREAT HUNTING

Initiatives such as Risk Monitoring and Risk and Vulnerability Assessment aim to reduce the dwell time and impact of cyberattacks by discovering and eliminating them before they cause significant damage or data breaches. All of them require a combination of human intelligence, analytical skills, and technical tools to identify and investigate suspicious activity, patterns, or anomalies that may indicate the presence of a threat.

Threat hunting is an essential component of a comprehensive and resilient cybersecurity strategy, as it complements and enhances the capabilities of automated security solutions and incident response teams.

PENETRATION TESTING (PT) & RED TEAMING (RT)

Penetration testing is a very effective security measure. This method involves a simulated cyberattack against a system or application to find and exploit its vulnerabilities by skilled and experienced ethical hackers who seek to breach a company's defenses.

A red team campaign is somewhat similar, but is a much broader assessment, testing a company's vulnerabilities and its response capabilities. Such a test, often conducted secretly with agreed scenarios, focuses on specific objectives rather than just findings and is a truly proactive approach.

"THIS IS ONLY RELEVANT FOR BIG COMPANIES"

This could not be further from the truth. Today, even smaller companies are data companies. Big companies invest in security solutions, which are proactive or not, but smaller companies often do not and are much easier to compromise. For attackers, these small businesses or individuals are "low hanging fruit" and widespread hybrid threats and more complex attacks available for purchase by amateur cybercriminals are very common. Small and midsize companies tend to be part of an extensive supply-chain of enterprises and if compromised, this can mean great danger to a company and their customers' security.

In conclusion, research data shows businesses that understand the benefits that proactive security brings to the table are significantly more ready in terms of cybersecurity. They understand that the goal of cybersecurity is not to prevent attacks, but rather to minimize the frequency and impact of attacks. With professional assistance, all businesses can reach that goal.

1 Report: Average time to detect and contain a breach is 287 days (venturebeat.com)
2 Why Human Error is #1 Cyber Security Threat to Businesses in 2021 (thehackernews.com)
3 Does phishing training work? Yes! Here's proof (www.cyberpilot.io)