CYBERSECURITY ASSESSMENT

HOW WELL IS YOUR ORGANIZATION SET UP REGARDING CYBERSECURITY?

IDENTIFYING GAPS IS THE FIRST STEP TO IMPROVING

Companies that fail at cybersecurity are in the news every day. For example, attackers steal confidential data, cripple your core systems, or encrypt your data to extort money. Regardless of the attackers' motivation or goal, the financial and reputational impact can be immense.

Therefore, the improvement of cybersecurity for your company is essential. You need to know the gaps and the corresponding risks. To mitigate these risks, an appropriate and secure posture is key to improving cybersecurity in any organization.

Necessary steps to improve cybersecurity:

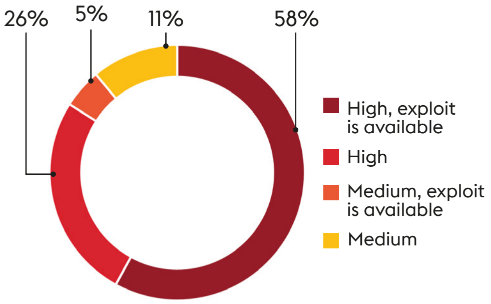
- Gain management attention
- Conduct cybersecurity assessment
- Identify and categorize gaps
- Identify and classify corresponding risks
- Define countermeasures
- Implement countermeasures
- Close gaps and minimize risks

With our fully comprehensive and proven assessment, we help you improve your organization's cybersecurity and mitigate risks.

OUR ADDED VALUE

- Cybersecurity professionals
- Many years working experience in the area of cybersecurity
- Relevant certificates:
  - CISSP (Certified Information Systems Security Professional)
  - CISA (Certified Information Systems Auditor)
  - Lead Auditor ISO/IEC 27001:2013
  - CompTIA Cyber Security Analyst (CySA+)
  - CompTIA Security+
  - CompTIA Network+
  - CompTIA Security Analytics Professional (CSAP)
  - CEH - Certified Ethical Hacker
  - ITIL v3 (Information Technology Infrastructure Library)
  - DoDD 85701 Tier 3 Certified Personnel

Severity of vulnerabilities and availability of exploits (percentage of companies):



© Positive Technologies
Own representation, according to: https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

Automotive · Aerospace · Railway · Energy · Life Sciences · Telecoms · Space · Services and Informations Systems · Defence · Oil and Gas · Consulting

THE BENEFITS OF A CYBERSECURITY ASSESSMENT

With a cybersecurity assessment, the first step to minimizing risks is done.

CUSTOMERS BENEFIT

- External assessment
- Document cybersecurity gaps
- Transparency of existing vulnerabilities
- Categorization of existing gaps
- Definition of next steps
- Increasing cyber resilience

RESULTS OF A CYBERSECURITY ASSESSMENT

- Management report
- Executive summary
- Detailed information including controls and their test results
- Countermeasures

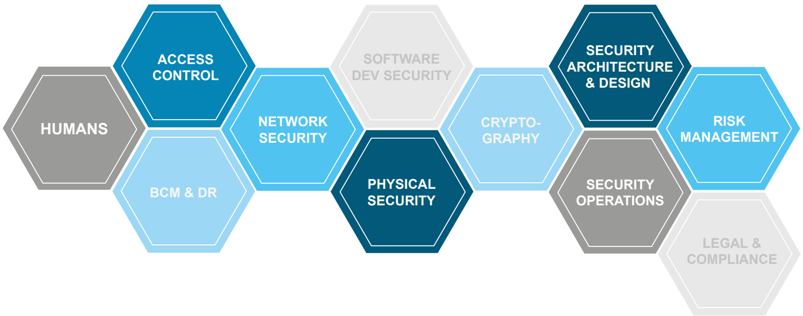
OUR CYBERSECURITY PORTFOLIO

The past shows that attackers don't care about the size of an organization. Cybersecurity has a vast range and focuses on many topics. Organizations know cybersecurity is essential, but they don't know what to do and how to start.

Our cybersecurity assessment is the first step to move forward, improve cybersecurity and minimize risks.

OUR APPROACH:

- Checklist oriented cybersecurity assessment
- Preferred onsite for about two days:
  - Interviews with the IT department
  - Selected interviews with staff not related to IT
  - Local inspection
  - Technical analysis of core IT components
  - Configuration evaluation of core IT components
  - Analysis of documentation and processes
- Documentation of all results
- Categorization of identified gaps
- Definition of countermeasures
- Presenting the final report


HUMANS
ACCESS CONTROL
BCM & DR
NETWORK SECURITY
SOFTWARE DEV SECURITY
PHYSICAL SECURITY
CRYPTO-GRAPHY
SECURITY ARCHITECTURE & DESIGN
SECURITY OPERATIONS
RISK MANAGEMENT
LEGAL & COMPLIANCE

AREAS IN FOCUS DURING A CYBERSECURITY ASSESSMENT:

- General IT security and password management
- Physical security
- IT management and the IT department
- User management
- Endpoint clients like laptops, PCs
- Server
- Local networks (LAN/VLAN)
- Wireless networks (WLAN)
- Printer
- Interfacing services
- Mobile devices like smartphone and tablet
- Employee, co-worker, and staff
- Cloud services