cryptware
secure your way

Solution Benefits:

- Daily vulnerability scans of your online systems
- 100% coverage of your public systems and continuous expansion is possible Immediate notification of critical (CVSS) vulnerabilities
- Detailed information on how to fix of the respective vulnerabilities
- Additional monthly overview reports with all results
- No access to your network required. Can be started immediately without customization
- 365 days a year as a subscription model
- For industry and medium-sized companies

Daily cyber Vulnerability Scans of all online assets

Every day, criminals scan and attack the entire Internet for vulnerable assets. They abuse more than 10,000 new vulnerabilities every year in standard software and operating systems. Sooner or later, every asset is concerned.
More than 10% of these vulnerabilities are, according to the definition of the industry standard CVSS, critical. Critical vulnerabilities allow attackers to take over complete control of your system and cause significant damage. Knowing whether your systems are affected by critical vulnerabilities is essential. In such cases to act quickly is necessary to fix the vulnerabilities before they are exploited. Our daily vulnerability scans by innoSec GmbH help you to stay ahead of the attackers.
You will notified immediately if your assets are affected by critical vulnerabilities. In addition, you will receive all necessary technical details to fix them quickly.

365

365 days/year

Scan of all assets

Immediate Alerting

Daily checks of your systems for vulnerabilities

Daily checks of all your public facing assets on the Internet, such as cloud solutions, firewall and proxy, web and mail server, VPN mail servers, VPN, DNS, SIP, IoT, home office etc. by market leading industry standard vulnerability scanner. It can detect configuration errors, insufficient patch levels, insecure services etc. can be detected. The vulnerabilities are classified, assessed and described in detail. Forgotten systems that become vulnerable over time are a

thing of the past. Just like overlooked patches and other avoidable errors that have already caused noticeable damage to to many companies. Translated with www.DeepL.com/Translator (free version)

Scope of service

Daily independent scan of your public accessible assets (by IP address or FQDN) for vulnerabilities. The scan is performed with a market-leading professional industry vulnerability scanner. If critical vulnerabilities are discovered, you will be notified immediately via email. The notification includes information about the vulnerability, its risk potential and recommended actions to fix it. In addition a complete report of all reviewed assets is delivered once a month, including also less critical vulnerabilities.

Scope of service

- Set-up costs incl.
- Initial scanning of all assets and creation of a complete report with all findings Daily scanning of all assets Monthly report of all found vulnerabilities
- Immediate email notification on discovery of critical vulnerabilities:

Optional (additional charge upon request)

- Coverage: Cyclic comparison of your DNS data DNS data with the assets to be scanned.
- Dedicated scan engines: E.g. for individual cloud connections Remediate: Remediation of the critical gaps
- Naming of the affected asset (IP or domain) Description of the critical vulnerability
- References to the critical vulnerability (if available, e.g., CVE). Recommendations for action (if possible, e.g. patch download link).

cryptware
secure your way

CryptWare IT Security GmbH
Frankfurter Str. 2
65549 Limburg

Phone: +49 (0) 6431 977790 - 0
Fax: +49 (0) 6431 977790 - 22
info@cryptware.eu

www.cryptware.eu

innoSec