Call Cheat Sheet

Lywand Software GmbH - lywand ['laɪvant] Wiener Dialekt
Synonym für großartig, hervorragend, sehr gut und gefallend

01 Herausforderung

+ KMUs geraten ins Fadenkreuz von Cyber-kriminellen – als primäres Angriffsziel oder als Teil der Lieferkette von Großunternehmen
+ Zusätzlich wachsende Angriffsfläche aufgrund von automatisierten Angriffen, Digitalisierung, Homeoffice und steigender Komplexität der ITInfrastrukturen
+ Security-Dienstleistungen und bereits vorhandene Produkte sind für KMUs oft zu teuer
+ Standardprodukte wie z.B. Antivirus und Firewall bieten keine umfassende Sicherheit
+ Fehlende Sichtbarkeit der eigenen IT-Sicherheitslage birgt Risiken

02 Lösung

Produktbeschreibung

Für KMUs bietet lywand vollautomatisierte und kontinuierliche IT-Sicherheitsüberprüfungen ihrer gesamten IT-Infrastruktur. Lywand schlägt Maßnahmen vor, die die IT-Sicherheit messbar erhöhen.

Funktionen

+ Automatisierte Security Audits der internen und externen IT-Infrastruktur
+ Einfache Bewertung sowie wichtige Keyfacts zur Sicherheitslage
+ Maßgeschneiderte Handlungsempfehlungen zur Verbesserung der IT-Sicherheit
+ Kompakter Report sowie Darstellung anhand einer Hausanalogie

03 Vorteile

+ Visibilität Ihrer IT-Sicherheitslage
+ Konkrete Sicherheitsmaßnahmen zur Minimierung Ihrer Angriffsfläche
+ Kontinuierliche Dokumentation der Security Audits
+ Unterstützung und Beratung von uns — wir übernehmen die Planung und Umsetzung der Maßnahmen

04 Security Check Details

Interner Agent Check

+ Ziele: Client & Server Endgeräte
+ Überprüfung auf bekannte Sicherheitslücken (CVE), Best-Practice Konfigurationen, Sicherheitsmechanismen sowie aktuelle Patchstände
+ Tägliche Überprüfungen, zusätzliche Checks möglich

Interner Netzwerk Check

+ Ziele: Ziele: Netzwerkgeräte (z. B. Laptops, Server, Drucker, Smartphones)
+ Ermittlung dieser Netzwerkgeräte mit Asset Discovery
+ Überprüfung auf Schwachstellen über das virtuelle Gateway
+ Laufende Checks & zusätzliche Checks möglich

Externer Check

+ Domänen, Subdomänen, IP Adressen und E-Mail Adressen
+ Überprüfung (z.B. Webserver, VPN Gateways) auf Sicherheitslücken und mögliche Einfallstore aus Sicht eines potenziellen Angreifers
+ Laufende & manuelle Checks möglich