Die automatisierte Security Audit Plattform für MSPs.

lywand software

Warum regelmäßige Audits entscheidend sind

Automatisierte Angriffe, Digitalisierung und die zunehmende Komplexität der IT-Infrastrukturen machen es immer schwieriger, den Überblick über die IT-Sicherheitslage zu behalten. Die Angriffsfläche wächst täglich und die fehlende Sichtbarkeit der IT-Sicherheitslage birgt Risiken. Eine einzelne Sicherheitslücke kann einem Hacker ausreichen, um unbemerkt in ein System einzudringen.

Die Funktionen im Detail

Mit lywand können Sie bei Ihren Kunden umfassende Sicherheitsprüfungen aus der Sicht eines potenziellen Angreifers durchführen:

- Die externe Infrastruktur, einschließlich (Sub-)Domains, E-Mail-Adressen und IP-Adressen, wird auf Schwachstellen analysiert. Zudem wird geprüft, ob gestohlene Unternehmensdaten im Darknet auftauchen.
- Die interne Infrastruktur, wie Laptops und Server, wird täglich auf bekannte Sicherheitslücken, Best-Practice-Konfigurationen und aktuelle Patchstände überprüft. Auch grundlegende Sicherheitsmechanismen wie die Windows Firewall und Antivirensoftware werden kontrolliert.
- Der Netzwerk Check analysiert alle Geräte im internen Netzwerk (wie Drucker, Smartphones und sonstige IoT-Geräte). So wird schnell erkannt, wo Schwachstellen und Konfigurationsfehler versteckt sind – oder wo es an notwendiger Systemhärtung fehlt.

Nach einem Security Audit wird die Sicherheitslage Ihrer Kunden übersichtlich dargestellt. Basierend auf den Ergebnissen gibt lywand konkrete Empfehlungen zur Behebung der Schwachstellen.

Beim nächsten Security Audit überprüft lywand, ob die Maßnahmen erfolgreich waren und die Sicherheitslücken geschlossen wurden. Die Ergebnisse werden kompakt und verständlich für Ihre Kunden in einem Management Report zusammengefasst.

Speicherung der Daten

Lywand legt alle Daten verschlüsselt in der Datenbank ab. Folgendes wird für den regulären Betrieb gesammelt:

- Ihre persönlichen Daten sowie Kundendaten, die im Zuge der Registrierung angegeben werden
- Identifizierte IT-Infrastrukturen & Sicherheitslücken
- Empfohlene Maßnahmen zur Behebung dieser Sicherheitslücken

Bereitstellung der Infrastruktur

Um IT-Security für alle einfach und auch kostengünstig zugänglich zu machen, läuft die Umgebung im Rechenzentrum von next layer in Wien (Österreich).

Dieses ist sowohl physisch als auch digital abgesichert und nach bewährten IT-Standards zertifiziert (ISO-27001, Code of Conduct für Internet Service Provider, ANKÖ LgU-Siegel, Bundesbeschaffung GmbH Partner, Cyber Trust Austria Silber Label). Details dazu können **hier** abgerufen werden.