

Sicherheitslage mit lywand bewerten und verbessern

Seit Jahren sieht sich die Wirtschaft einer wachsenden Zahl an Cyber-Angriffen ausgesetzt. Umso wichtiger ist es daher für Unternehmen, einen ausführlichen Überblick der eigenen Sicherheitslage zu bekommen, sich zu wappnen und entsprechende Maßnahmen im Bereich der Cybersecurity zu setzen.

Lywand bewertet einfach, schnell, verständlich, kontinuierlich und kostengünstig die aktuelle Sicherheitslage der digitalen Infrastruktur Ihrer Kunden und zeigt Schritt für Schritt auf, wie Sie diese verbessern können.

Funktionen des lywand Dienstes im Detail

Lywand identifiziert und überprüft automatisiert die externe Infrastruktur (Domänen, IP Adressen und E-Mail Adressen). Die interne Infrastruktur (Endgeräte und Server) wird mittels Agents täglich überprüft. Dieser Agent läuft dabei unbemerkt im Hintergrund und bleibt mithilfe von Auto-Update immer am neuesten Stand.

Nach dem Starten des Sicherheits-Checks können Sie gespannt auf die Bewertung der Infrastruktur warten. Dies kann je nach Größe des zu überprüfenden Bereiches eine Weile dauern. In dieser Zeit koordiniert lywand verschiedenste Module (Schwachstellenscanner und Systeme zur Erkennung der Veröffentlichung von Benutzerdaten), welche die Infrastruktur auf Sicherheitslücken überprüft.

Im Anschluss daran wird der Sicherheitszustand des überprüften Unternehmens auf einfache Art und Weise visuell dargestellt. Bereits priorisierte Maßnahmen sollen Ihnen dabei helfen, an den wichtigsten Schrauben zuerst zu drehen. Die vorgeschlagenen Maßnahmen können anschließend von Ihnen in einem sogenannten „Renovierungsplan“ geplant werden. Dieser dient als konkrete Checkliste um die identifizierten Probleme zu beheben. Nach der Umsetzung der Maßnahmen kann die gesamte Infrastruktur erneut überprüft werden, um so die Verbesserung der Sicherheit mit lywand ersichtlich zu machen.

Speicherung der Daten

Lywand sammelt folgende Daten für den regulären Betrieb:

- + Ihre persönlichen Daten sowie Kundendaten, welche im Zuge der Registrierung angegeben werden.
- + Informationen, welche über öffentlichen Datenquellen ermittelt werden. Einerseits die identifizierte Infrastruktur der Unternehmensumgebung, welche sich aus den gefundenen Zielen zusammensetzt. Andererseits die identifizierten Sicherheitslücken der überprüften Infrastruktur.
- + Maßnahmen, welche von Ihnen zur anschließenden Umsetzung geplant werden.

Alle Daten werden verschlüsselt in der Datenbank abgelegt.

Bereitstellung der Infrastruktur

Unsere Mission ist es, IT-Security für alle einfach und auch kostengünstig zugänglich zu machen. Um dies zu garantieren, läuft unsere Umgebung in einer hochverfügbaren sicheren Private Cloud in Frankfurt (Deutschland). Das Rechenzentrum ist sowohl physisch als auch digital abgesichert und nach bewährten IT-Standards (Zertifizierungen ISO 27001, ISO 27017, ISO 27018, PCI DSS, uvm.) zertifiziert. Details dazu können [hier](#) abgerufen werden.