HCLSoftware

Die Sicherheit aller Endgeräte in die eigene Hand nehmen

Rik Kornelson
Product Specialist - Intelligent Operations

+49 172 602 13 76
Rik.Kornelson@hcl-software.com

Top Herausforderungen

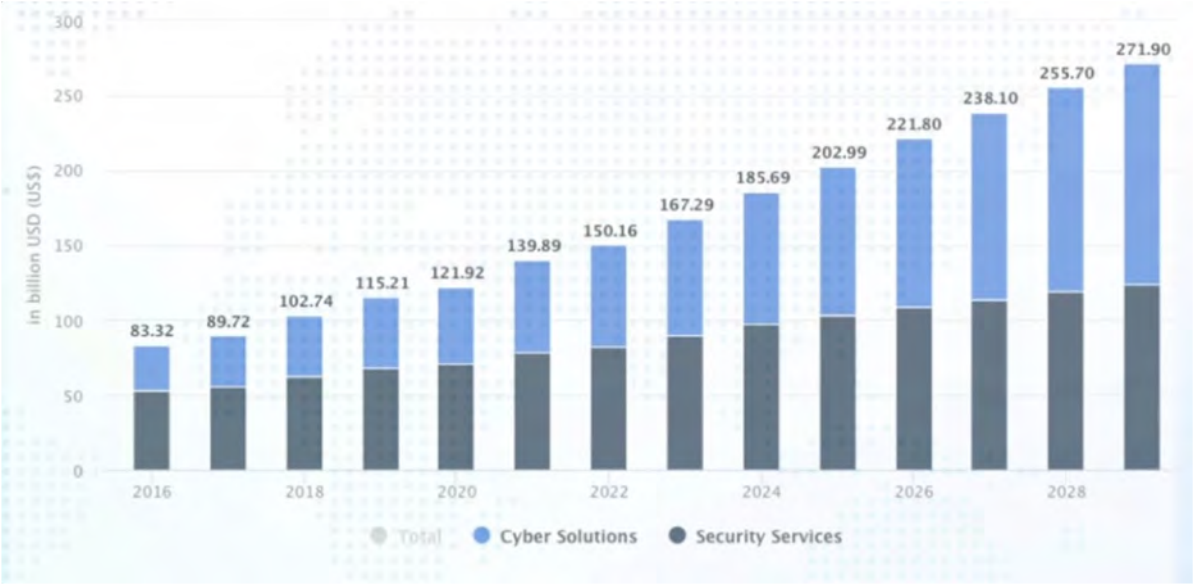
1. Cybersecurity
2. Digitale Innovation
3. Investitionsentscheidungen

Source: Diligent Institute , What Directors Think“

Es werden Rekordsummen in Cybersecurity investiert

$ 185 Mrd.
wurden schon 2024 in Cybersecurity investiert

$ 271 Mrd.
werden 2029 in Cybersecurity investiert

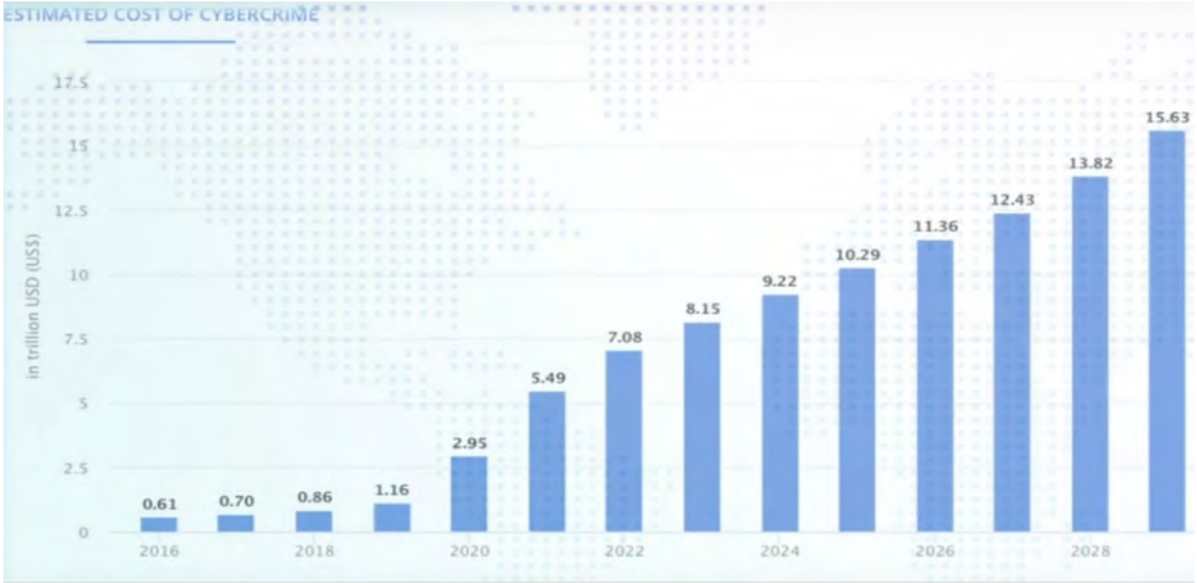


Source: Statista Market Insights

Cybercrime verursacht aber deutlich mehr Kosten

Cybercrime
kostet uns 2024
$ 9,22 Billionen

...und es wird für 2029 ein
Wachstum vorausgesagt auf
$ 15,63 Billionen



Source: Statista Market Insights

Von wem werden wir angegriffen?

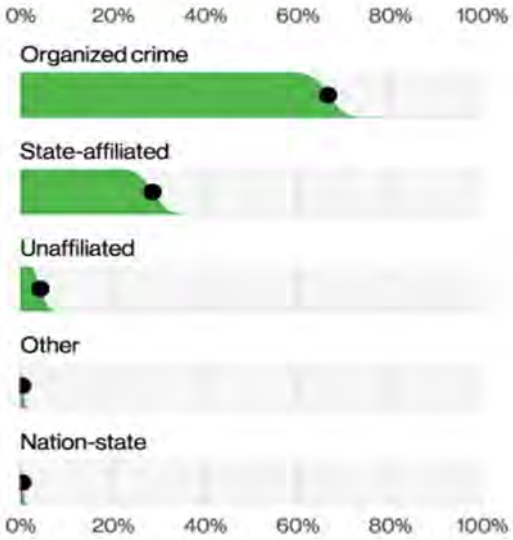


Figure 73. Top External actor varieties in Public Administration industry breaches (n=305)

Source: Verizon Data Breach Investigation Report

Erster Platz 2024
Organisiertes Verbrechen

Zweiter Platz 2024
staatliche Angreifer

Was sind die Motive für Cybersecurity-Angriffe?

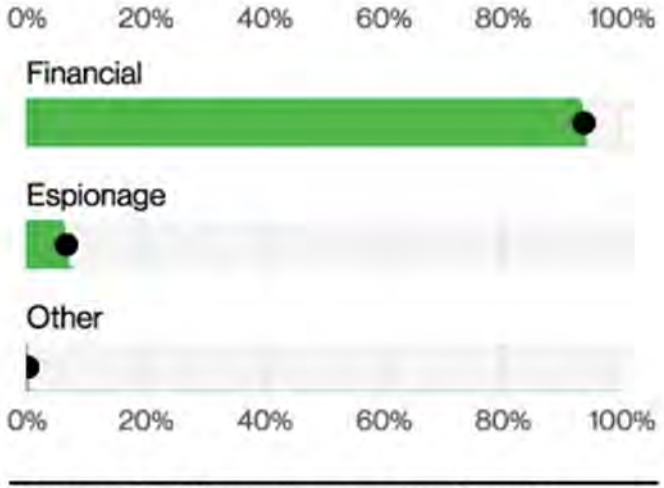


Figure 12. Threat actor motives in breaches (n=5,632)

Source: Verizon Data Breach Investigation Report

Finanzielle Motive:

92%

in 2024

Spionage als Motiv:

7%

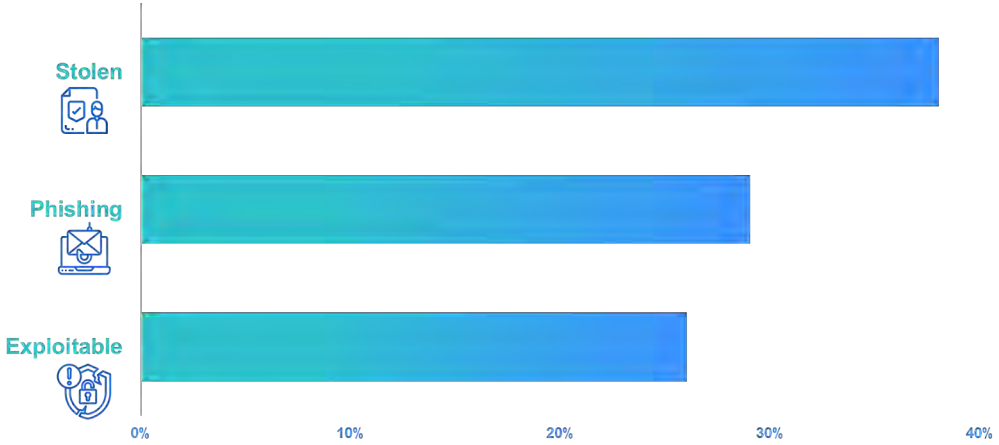
in 2024

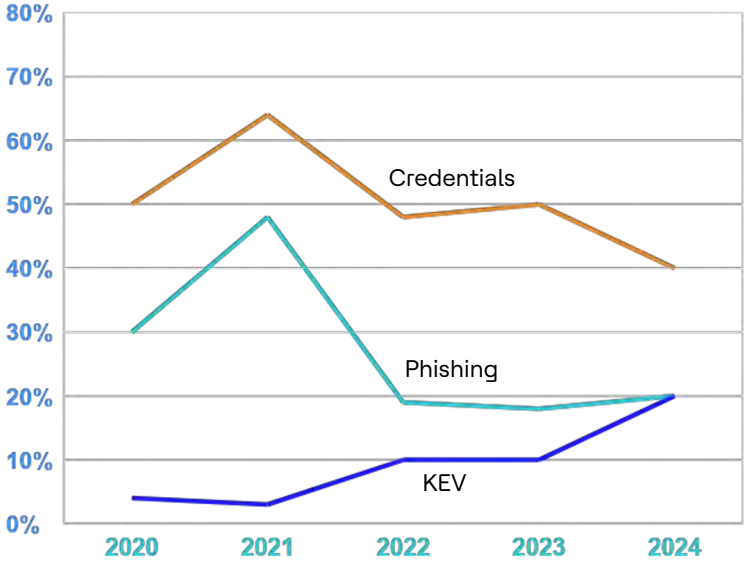
3 Hauptwege führen in Ihre Infrastruktur

- Gestohlene Zugangsdaten
- Phishing
- Bekannte, ausgenutzte Schwachstellen (KEV)

Source: Verizon Data Breach Investigation Report

Werden KEVs in der Zukunft die vorherrschende Bedrohung?





Source: Verizon Data Breach Investigation Report

Gestohlene Zugangsdaten und Phishing sind nach wie vor vorherrschende Angriffsmethoden, aber

Known Exploitable Vulnerabilities (KEV) werden zum Hauptangriffsweg

Neue Schwachstellen wachsen massiv

Beachtlicher Anstieg von 2019 auf 2020

Wird AI die Situation verbessern?

Source: Statista Market Insights

92% der Entwickler nutzen derzeit AI-Codingtools

Source: Github Survey

Organisationen benötigen 55 Tage um 50% der „CISA KEV" Schwachstellen zu beseitigen

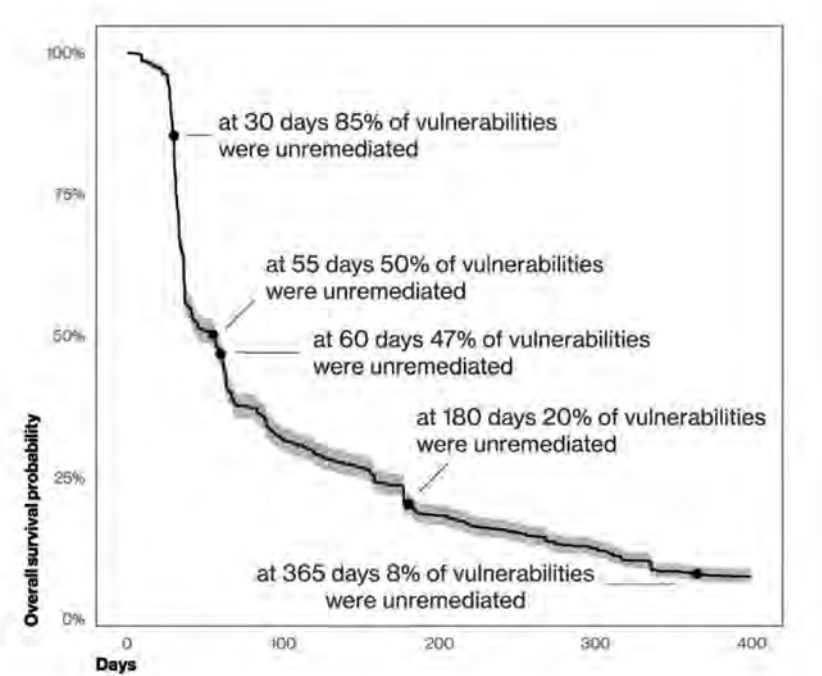


Figure 19. Survival analysis of CISA KEV vulnerabilities

Source: Verizon Data Breach Investigation Report

Ein Angreifer benötigt im Durchschnitt aber nur wenige Stunden

Durchschnittlich treten Attacken für „new exploits identified" nach 12 – 18 Stunden auf.

2024 waren es noch durchschnittlich 4,76 Tage.

Viele Unternehmen patchen nicht effektiv

… und sie wissen das auch …

60% der Schäden passieren, obwohl der Patch verfügbar war, aber nicht ausgerollt wurde

nur 9% der befragten Unternehmen gaben an, dass sie effektiv Schwachstellen beheben

Source: The State of Vulnerability Management, Survey by Tenable and BigFix,

Mögliche Lösungsansätze

Beschleunigung

..die Zahl der wichtigen Cyber-Sicherheitsmaßnahmen zu erhöhen, die wir in der gleichen Zeit wie bisher durchführen können, ohne darüber nachzudenken oder mehr Aufwand zu betreiben.

Zusammenarbeit

...die Lücken zwischen Sicherheit, IT und der Führungsebene zu schließen.

Finden Sie Wege zur Messung von Cyber Risiken und zur Kontrolle von Sicherheits-Ergebnissen mit Hilfe von Werkzeugen und Prozessen.

Konsolidierung

...vereinfachen Sie Prozesse durch die Nutzung der richtigen Tools und brechen Sie die Silos auf..

Das typische Unternehmen nutzt zwischen 4 bis 14 Tools für die Endpoint Security.

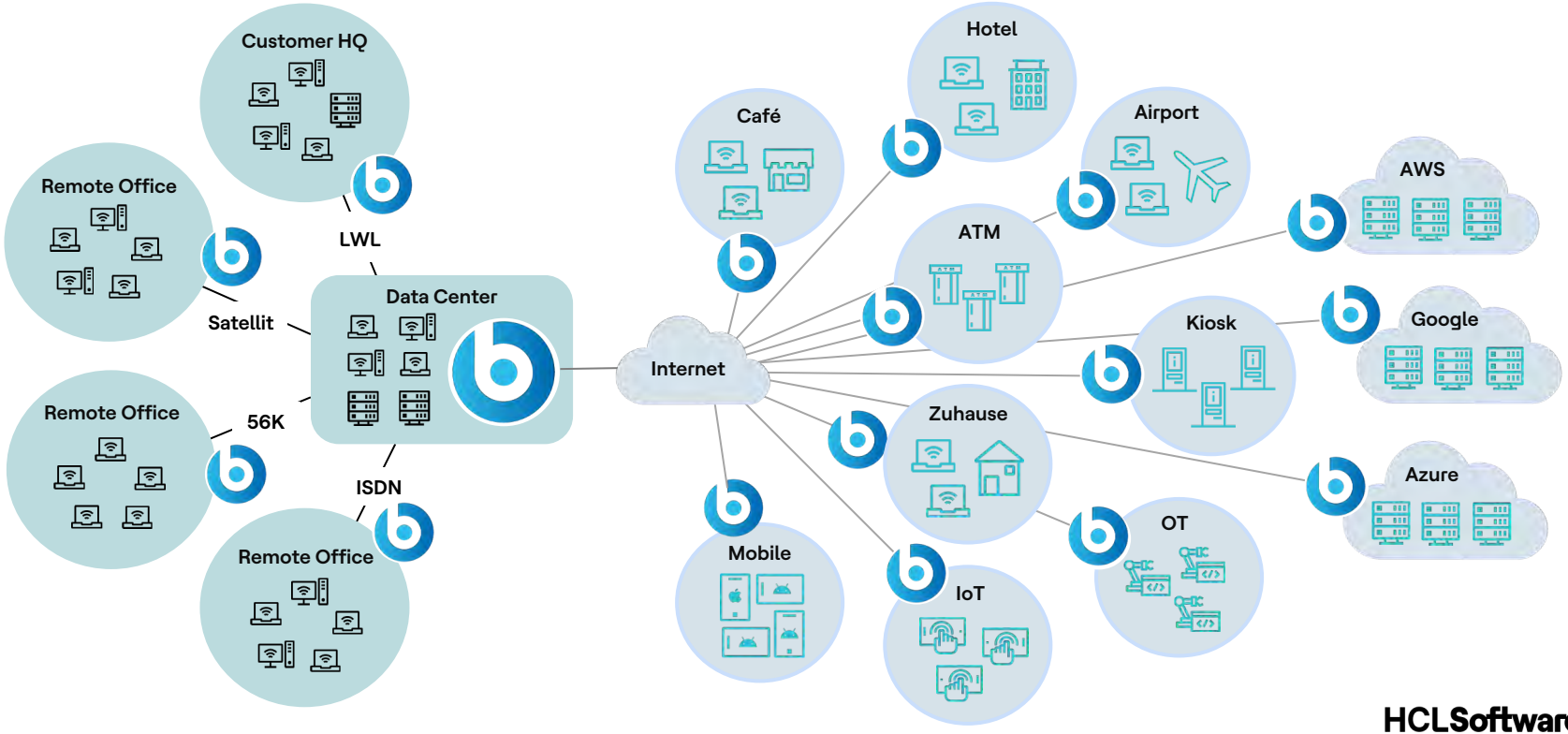
HCL BigFix

Cybersecurity

HCLSoftware

Wahre Souveränität entsteht nur durch Transparenz und Klarheit

HCL BigFix findet, verwaltet und sichert alle Endpoints



HCLSoftware

CYBERSECURITY

So hilft HCL BigFix

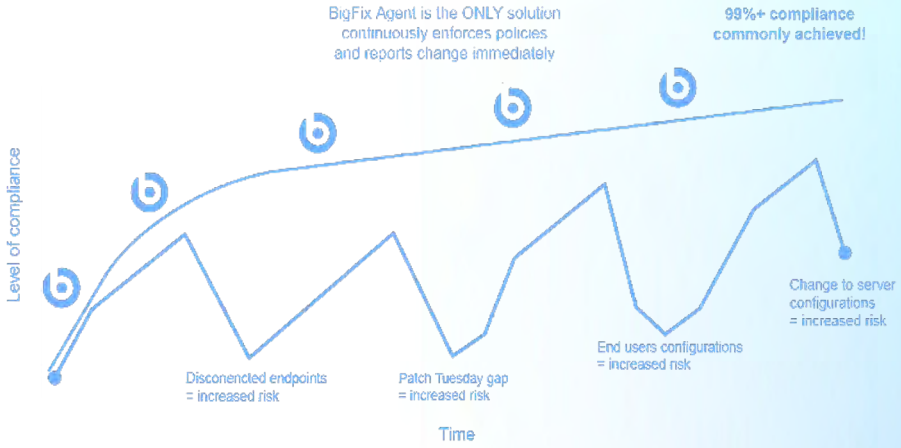
Herausforderungen	**Sicherheitslücken zu lange offen**	**Zu viele Tools und Software-Agents**	**Keine Sichtbarkeit**	**Personalmangel**	**Compliance-Vorgaben**
	1/3 der Schwachstellen sind nach einem Jahr noch nicht behoben	Eine typische Organisation verwendet 14 Tools	Sicherheitsrisiko durch fehlende konsolidierte Management-Sicht	2025 waren 4 Mio. Jobs im Bereich Cyber Security unbesetzt	Bei Verstößen drohen Millionenstrafen
Lösung mit BigFix	**Schnelle Behebung von Schwachstellen**	**Nur eine Software mit einem Software-Agent**	**Einheitliche Sicht**	**Einfacheres Staffing**	**Durchgängige Compliance**
	Priorisiert, beschleunigt, automatisiert die Behebung	BigFix bekämpft Wildwuchs und reduziert Komplexität	Eine zentrale Sicht vereinfacht Kontrolle und reduziert Risiken	Ein Skillset für alle Betriebssysteme und Gerätetypen	verhindert Configuration Drift und Nichteinhaltung von Vorschriften
Resultat	**Weniger Sicherheitsrisiken**	**Niedrigere IT-Kosten**	**Verbesserte Sichtbarkeit und Kontrolle**	**Freie IT-Ressourcen**	**Weniger Strafen für Non-Compliance**

HCLSoftware

Resilienz durch Automatisierung: Souveränität im Dauerbetrieb.

BigFix prüft kontinuierlich alle Richtlinien und Konfigurationen auf den Endpoints und stellt sicher, dass diese regelkonform sind:

- ✓ Bewertung nahezu in Echtzeit
- ✓ Korrektur von Konfigurationsabweichungen
- ✓ Analyse und Reporting; historische Trends



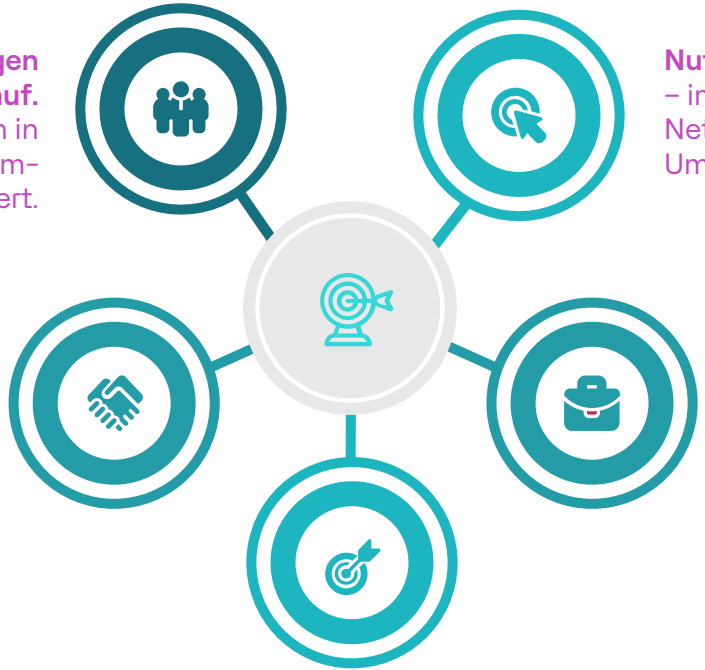
HCL BigFix hilft mehr als 1.500 Kunden bei der Einhaltung kritischer Compliance wie HIPAA, NIS2, DORA, CIS, CISA-Kev, DISA STIG, NIST, PCI-DSS, RBI, ISO-27001 etc.

CYBERSECURITY

Ob On-Premises, Hybrid oder in der souveränen Cloud HCL BigFix garantiert volle Kontrolle über Ihre Infrastruktur

Hohe Patch-Effizienz mit einer 98%-igen Erfolgsrate im ersten Durchlauf. Schließen Sie kritische Sicherheitslücken in Stunden statt Wochen, betriebssystem-übergreifend und automatisiert.

Lückenlose Software- und Hardware-inventarisierung: Erkennung von 100.000+ Produkten. Bekommen Sie Ihre Schatten-IT wieder unter Ihre Kontrolle, egal an welchem Standort.



Nutzen Sie BigFix dort, wo Sie es brauchen – im eigenen Rechenzentrum, in hybriden Netzen oder in einer souveränen Cloud-Umgebung.

Ein Agent, eine Konsole, alle Welten. Ersetzen Sie isolierte Einzellösungen durch eine einheitliche Plattform für das gesamte Endpoint-Management.

Revisionssicherheit durch kontinuierliches Monitoring: Vermeiden Sie Bußgelder und erfüllen Sie Mandate wie NIS-2/CIS auf Knopfdruck.

HCLSoftware

HCLSoftware

hclsw.de