ivanti

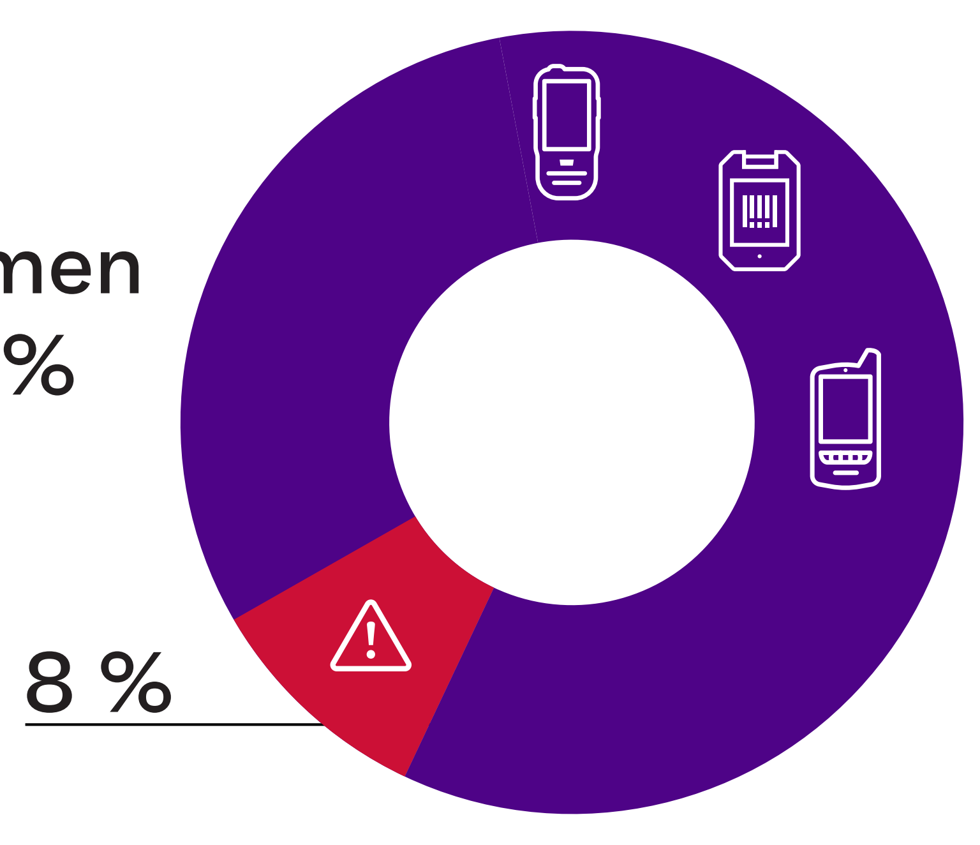
Fünf Dinge, die beim Management von Sicherheitslücken behoben werden müssen

1 Ihre blinden Flecken in Sachen Sicherheitslücken

Man kann nicht schützen und patchen, was man nicht sehen kann – oder wissen, worauf man achten muss.

1 von 3 Mitarbeitern in Fortune-1000-Unternehmen verwenden nicht genehmigte cloudbasierte SaaS-Anwendungen.(i)

Drei der beliebtesten Scanner – Nessus, Qualys und Nexpose – **übersehen zusammen immer noch fast 8 %** aller bekannten Ransomware-Sicherheitslücken.(ii)



2 Mangelnde Teamkapazität

Stellen Sie sich vor, Sie müssten versuchen, jede Schwachstelle oder jedes Risiko zu schließen – oder nur die Schwachstellen manuell überprüfen, die für Ihr Unternehmen und Ihre Umgebung am wichtigsten sind.

⚠
Über 236.000 kritische Schwachstellen und Gefährdungen (CVEs) insgesamt

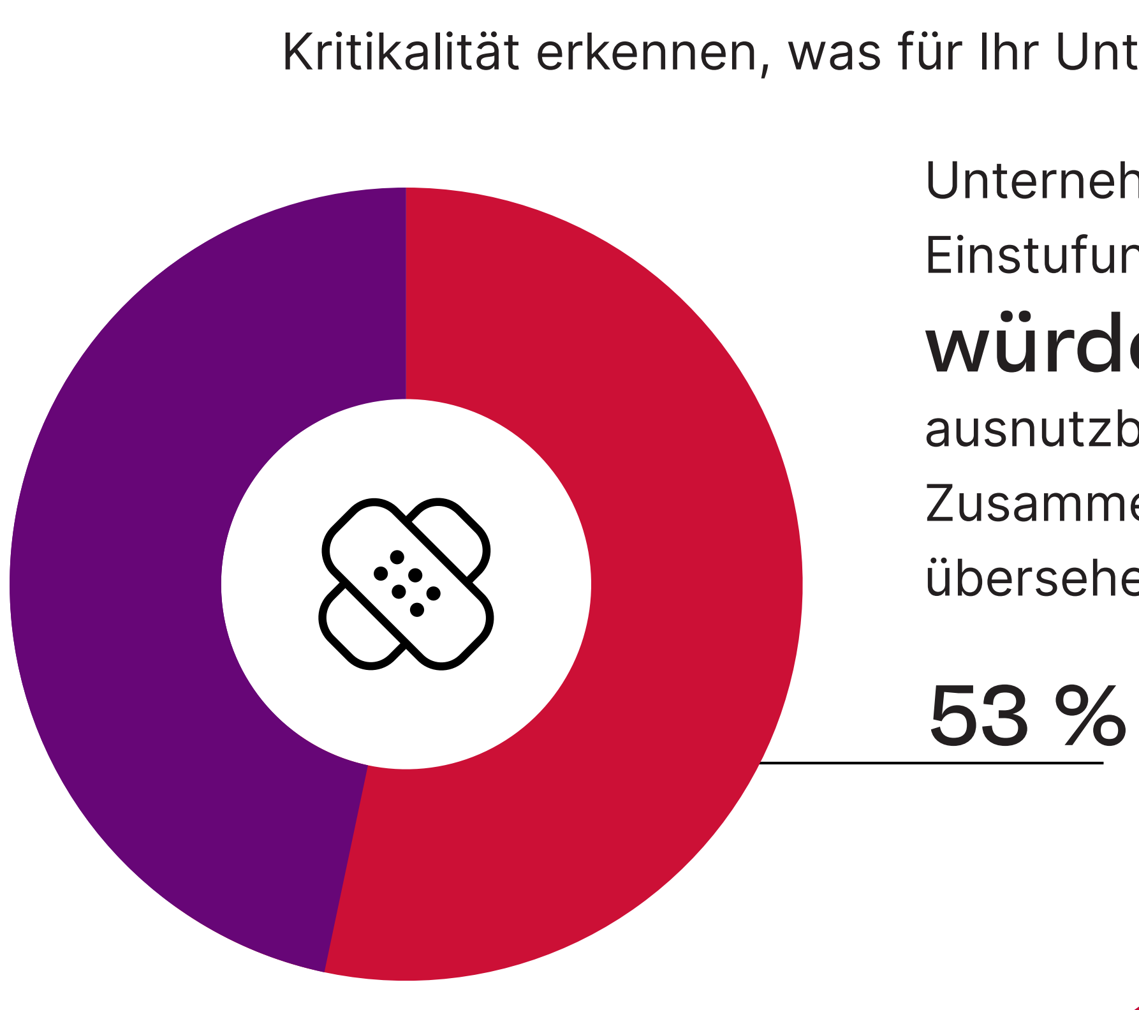
⚠ ⚠
Über 29.000 für Angriffe genutzte CVEs

⚠ ⚠ ⚠
Über 9.600 CVEs mit Möglichkeiten zur Remote Code Execution (RCE) und/oder Privilege Escalation (PE)

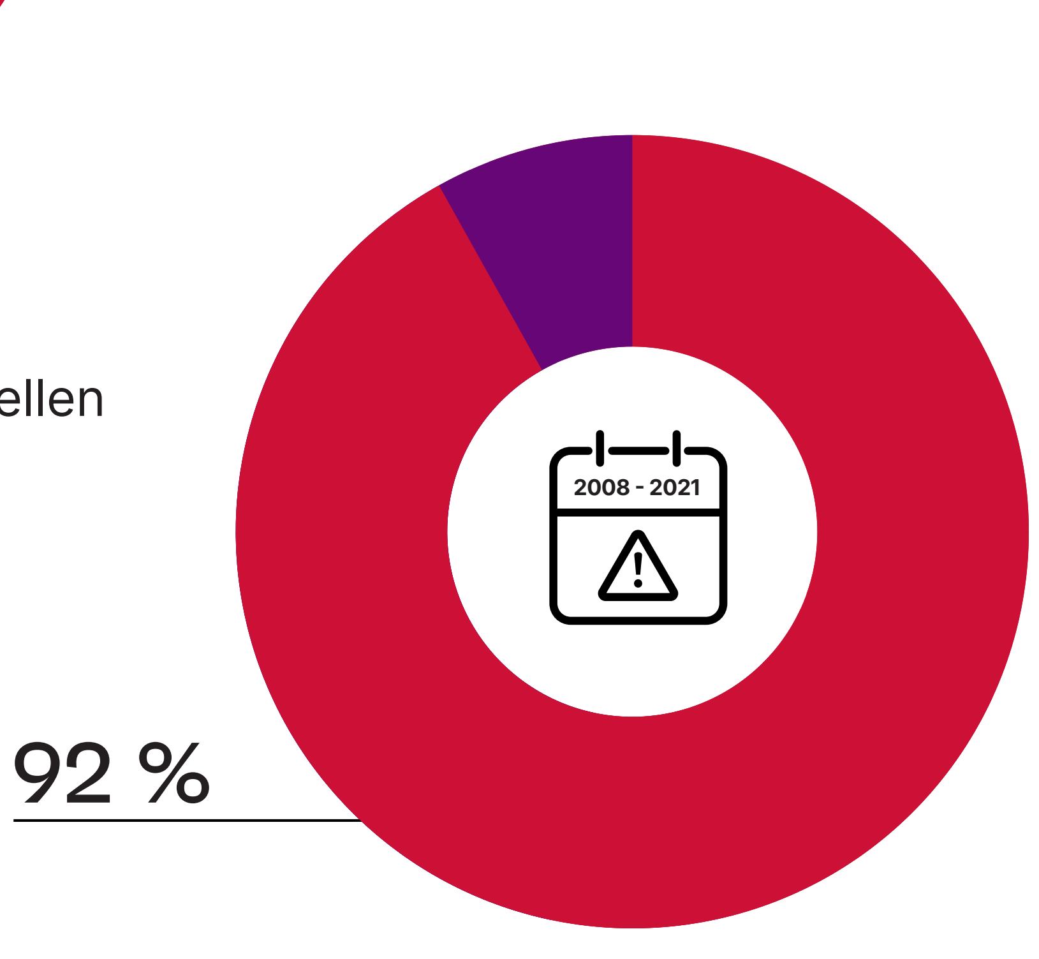
3 Anfälligkeit für weniger „kritische“ und ältere CVEs

Nicht alle Schwachstellen stellen das gleiche Risiko dar – und Sie können nicht allein anhand des Alters oder der Kritikalität erkennen, was für Ihr Unternehmen relevant ist.

Unternehmen, die nur CVEs mit der Einstufung „kritisch“ patchen, **würden 53 % aller** ausnutzbaren Schwachstellen im Zusammenhang mit Ransomware übersehen.(iii)



92 % aller aktiven Schwachstellen sind älter als ein Jahr – einige wurden erstmals 2008 veröffentlicht![iv]



4 Wenige Programmressourcen und geringe interne Akzeptanz

Basis-RBVM

Prioritätensetzung durch CVSS-Scores und Scanner-Scores

Schwachstellen
Hängt stark von der Datenqualität und der Häufigkeit der Scanner-Updates ab

Schwachstellen mit geringerer Bewertung, die für organisationsspezifische Risiken relevant sind, werden übersehen

Stärken
Es gibt ein Schwachstellenmanagement

Mittleres RBVM

Prioritätensetzung durch Ausnutzungswahrscheinlichkeit der CVEs des letzten Jahres

Schwachstellen
Erfordert ständige manuelle Abstimmung und Überprüfung

Verpasst noch relevante ältere Schwachstellen (älter als 1 Jahr)

Stärken
Priorisierung von Abhilfemaßnahmen über CVSS-Score hinaus

Neue Schwachstellen werden hervorgehoben

Fortgeschrittenes RBVM

Priorisierung durch Multi-Sourced Threat Intelligence und kontextualisierte Unternehmensrisiken

Schwachstellen
Erfordert eine umfassende Tool-Suite zur Abdeckung mehrerer Datenquellen

Stärken
Enthält alle möglichen Quellen von Daten über Sicherheitslücken

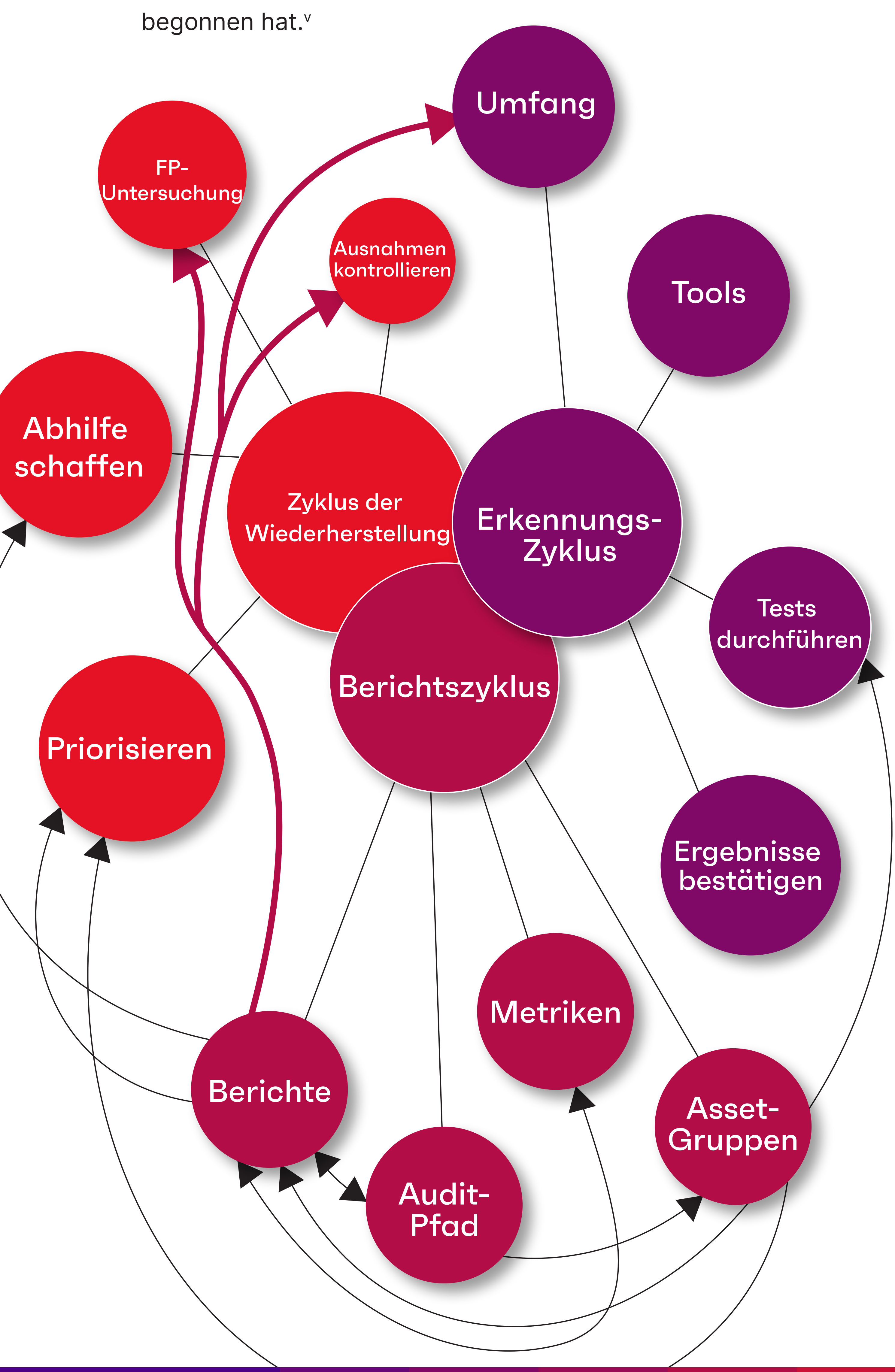
Setzt Prioritäten auf der Grundlage einzigartiger organisationsspezifischer Risiken

Schnelles Umschwenken, um neue Zusammenhänge zu berücksichtigen und die Prioritäten zu verfeinern

5 Berichte

Effektive Programme zur Verwaltung von Schwachstellen können schnell ein verworrenes Geflecht aus abteilungsübergreifenden Erkennungs-, Behebungs- und Berichterstattungsmaßnahmen bilden, die für eine ordnungsgemäße Ausführung erforderlich sind.

Ohne ein Automatisierungstool, das Informationen über Schwachstellen und Aktivitäten zusammenfasst, nach Prioritäten ordnet und anzeigt, könnte Ihr Cybersicherheitsprogramm an den Berichterstattungsanforderungen scheitern, bevor es überhaupt begonnen hat.[v]



Das muss nicht so sein. Lesen Sie den Spotlight Ransomware Report 2022, um sich über die neuesten Sicherheitslücken zu informieren.

Bericht herunterladen

---

i “Why shadow IT is the next looming cybersecurity threat” (The Next Web)
ii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iii Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
iv Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
v OWASP Vulnerability Management Guide (OVMG) - June 1, 2020

IVI-2706 06/22 FG