Audit vom 20.06.24, 06:10:48

GERARD
IT-STRUKTUREN EINFACH VERNETZEN

IT-SECURITY AUDIT

Audit-Report des automatisiert durchgeführten Penetrationstest

Durchgeführt von:

Klassifizierung: Streng vertraulich

Hinweise

Enginsight® evaluiert und bewertet die Sicherheit Ihrer Unternehmens-IT-Infrastruktur. Dabei werden die definierten Zielsysteme geprüft und bewertet. Die Bewertung basiert auf den von Enginsight® geprüften Sicherheitskriterien, die angelehnt sind an technische Empfehlungen und Branchenstandards, wie z. B. vom BSI, MITRE ATT&CK® oder der VdS. Die Bewertung enthält keine organisatorischen Elemente. Die Bewertung stellt eine Momentaufnahme der aktuellen Angreifbarkeit der IT-Infrastruktur dar. Die Angriffslage und damit auch die Angreifbarkeit können sich jedoch jederzeit ändern. Enginsight® stellt keine vollumfängliche Risikobewertung für Cyberattacken dar, sondern zeigt die IT-Angreifbarkeit aus Sicht eines Cyberkriminellen. Somit ist die Durchführung des Enginsight® Audits als Bestandteil einer umfänglichen Risikoanalyse anzusehen, die die Cyberrisiken Ihres Unternehmens ganzheitlich bewertet.

Vertraulichkeitserklärung

Dieses Dokument ist das ausschließliche Eigentum von XXX und Enginsight®. Dieses Dokument enthält geschützte und vertrauliche Informationen. Die Vervielfältigung, Weitergabe oder Verwendung, ganz oder teilweise, in jeglicher Form, erfordert die Zustimmung sowohl der XXX als auch von Enginsight®. XXX darf dieses Dokument im Rahmen von Vertraulichkeitsvereinbarungen an Prüfer weitergeben, um die Einhaltung der Penetrationstestanforderungen nachzuweisen.

Disclaimer

Der Autor übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.

Definition der Schweregrade

In der folgenden Tabelle sind die Schweregrade definiert, die im gesamten Dokument zur Bewertung der Schwachstellen und der Auswirkungen des Risikos verwendet werden.

CRITICAL	Die Ausnutzung der Schwachstellen ist einfach und führt in der Regel zu einer Beeinträchtigung der Systemebene, Datenverlust oder Ausfallzeiten. Es wird empfohlen, einen Aktionsplan zu erstellen, um die Schwachstelle umgehend zu beheben.
HIGH	Eine Ausnutzung der Schwachstelle ist schwieriger, kann aber zu erhöhten Berechtigungen und möglicherweise zu Datenverlusten oder Ausfallzeiten führen. Es wird empfohlen, einen Aktionsplan zu erstellen, um die Schwachstelle zeitnah zu beheben.
MEDIUM	Schwachstellen, die nicht ohne weitere Maßnahmen, wie z.B. Social Engineering ausgenutzt werden können.
LOW	Die Schwachstellen sind nicht unmittelbar ausnutzbar. Ein Beheben würde aber die Angriffsfläche Ihrer Organisation verringern.

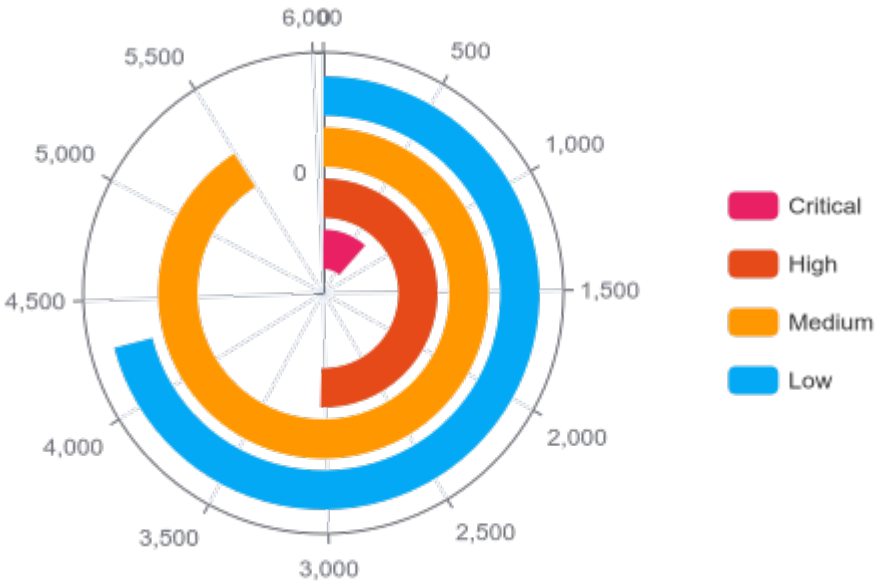
Managementübersicht

Die Managementübersicht bietet einen Überblick über identifizierte Risiken, die Anzahl der Ergebnisse und deren Schweregrade. Der Risikoscore macht regelmäßige Audits vergleichbar und zeigt die Risikoentwicklung über die Zeit. Ein kontinuierlicher Rückgang des Risikoscores deutet auf effektive Maßnahmen zur Schwachstellenbehebung und Härtung der IT-Infrastruktur hin. Regelmäßige Überwachung und Anpassung dieser Maßnahmen sind essentiell für die stetige Verbesserung der Systemintegrität und -sicherheit.

Schwachstellen nach Schweregrad

Im Audit wurden insgesamt 13517 Schwachstellen identifiziert. Diese lassen sich wie folgt in verschiedene Schweregrade einteilen:

CRITICAL	HIGH	MEDIUM	LOW
694	3045	5493	4285



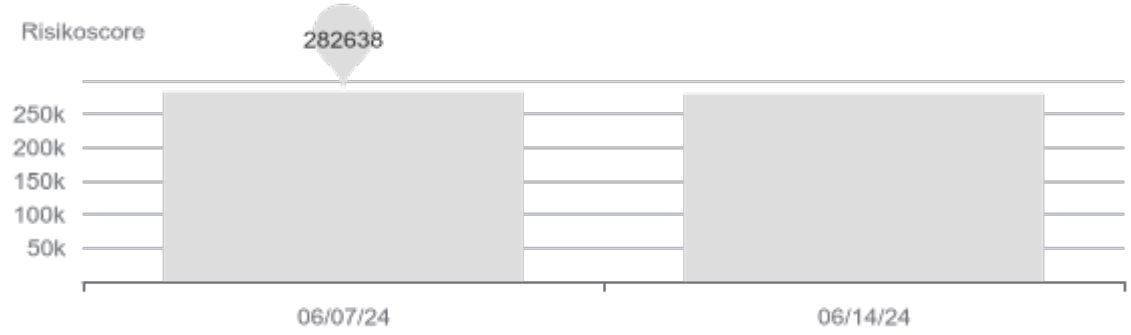
Kalkulierter Risikoindex

Ein Risikoscore, basierend auf der Anzahl und dem Schweregrad der gefunden Ergebnisse, wobei kritische Schwachstellen stärker gewichtet werden. Er ermöglicht den Vergleich von Audits und die Bewertung der umgesetzten Maßnahmen. Das Ziel sollte immer sein, den Score dauerhaft zu senken, um die Sicherheit und Integrität des Systems fortlaufend zu erhöhen.

Aktueller Risikoscore	280865	Letzter Risikoscore	280865

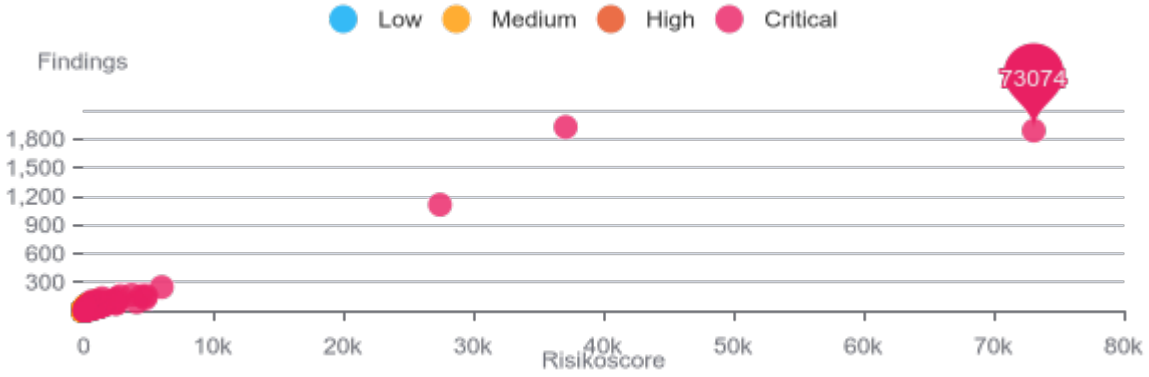
Risikowerte im Zeitverlauf

Wiederholte Audits nach einer definierten Vorgabe zeigen die Entwicklung des Risikowerts über die Zeit. Eine kontinuierliche Reduktion dieses Wertes deutet auf effektive Sicherheitsmaßnahmen und verbesserte Systemintegrität hin, was das Hauptziel der Audits immer sein sollte.



Top 20 der gefährdetsten Ziele

Im Diagramm werden die Top 20 Ziele mit dem höchsten Risikowert dargestellt. Diese Visualisierung hebt die kritischsten Ziele hervor, die im Rahmen des Audits identifiziert wurden.



Analysierte Ziele

Die Zielsysteme, die sich aus dem definierten Bereich ergeben, sind hier aufgelistet. Bei größeren Tests ist es üblich, dass nicht alle Zielsysteme zum Zeitpunkt des Audits erreichbar sind; daher sind in dieser Liste nur die Systeme aufgeführt, die zugänglich waren und getestet wurden, sortiert nach Schweregrad.

Ziel	Ergebnisse	Risikoscore	Schweregrad
192.168.200.123	1887	73074	CRITICAL
192.168.203.214	1925	37093	CRITICAL
192.168.201.60	1111	27434	CRITICAL
192.168.201.26	248	6050	CRITICAL

Ziel	Ergebnisse	Risikoscore	Schweregrad
192.168.201.34	158	4868	CRITICAL
192.168.201.35	128	4775	CRITICAL
192.168.201.31	156	4506	CRITICAL
192.168.201.162	90	4118	CRITICAL
192.168.201.28	167	3749	CRITICAL
192.168.203.213	155	2865	CRITICAL
192.168.201.158	130	2605	CRITICAL
192.168.201.161	76	2562	CRITICAL
192.168.201.48	102	2514	CRITICAL
192.168.201.250	75	2497	CRITICAL
192.168.201.100	110	2277	CRITICAL
192.168.201.70	89	1834	CRITICAL
192.168.200.140	89	1629	CRITICAL
192.168.201.59	58	1610	CRITICAL
192.168.201.55	132	1471	CRITICAL
192.168.201.219	63	1462	CRITICAL
192.168.201.252	96	1435	CRITICAL
192.168.201.98	75	1312	CRITICAL
192.168.201.1	55	1309	CRITICAL
192.168.202.17	44	1297	CRITICAL