itk - Vektoranalyse

1 Einführung in die ITK-Vektoranalyse

Unser Ziel ist es, mit einer umfassenden Gesamtlösung einen klaren Überblick zu schaffen, um den Status sowie die notwendigen Maßnahmen für einen dauerhaft sicheren Betrieb der Unternehmens-IT zu gewährleisten.

2 Was ist ITK-Vektoranalyse?

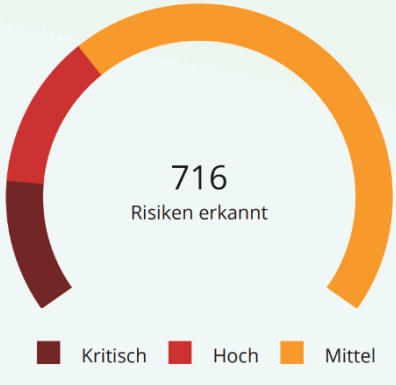
Die ITK-Vektoranalyse bietet eine hochentwickelte und bewährte Methode zur Bewertung der Cybersicherheitslandschaft eines Unternehmens. Durch die Kombination interner und externer Penetrationstests ermöglicht sie eine gründliche Untersuchung der gesamten IT-Infrastruktur. Dabei werden nicht nur sämtliche verbundenen Hardware- und Softwarekomponenten identifiziert, sondern auch potenzielle Sicherheitslücken aufgedeckt.

Die Ergebnisse liefern klare Handlungsempfehlungen zur Behandlung von IT-Sicherheits-risiken. Diese ganzheitliche Analyse befähigt Unternehmen, ihre Sicherheitsmaßnahmen gezielt zu verstärken und regulatorische Anforderungen, wie etwa die des Bundesamts für Sicherheit in der Informationstechnik (BSI) zum Beispiel im Kontext der KRITIS oder NIS 2.0 Vorgaben, effizient zu erfüllen.

Risikoübersicht

Die Gesamtanzahl, der bei der Bewertung entdeckten, Sicherheitsrisiken wird nach Art und Schweregrad aufgeführt:

Kritisch	Hoch	Mittel
Dies bezeichnet bestätigte bösartige Payloads, die ausgeführt wurden, oder ein sehr hohes Maß an Gefährdung durch einen Cyberangriff darstellen.	Dies deutet auf latent vorhandene Malware hin, die jederzeit ausgeführt werden könnte, oder die dringende Notwendigkeit, die Angriffsfläche zu verkleinern.	Hierbei handelt es sich um zusätzliche Risikofaktoren, die präventiv angegangen werden sollten.



3 Von Innen nach Außen

Etwa 80% aller Cybersecurity-Angriffe erfolgen über bereits kompromittierte Geräte innerhalb des Unternehmensnetzwerks und nicht von außen! Unser einzigartiger Ansatz zur ITK-Vektoranalyse unterscheidet sich von herkömmlichen Methoden durch die Integration externer und interner Sicherheitsprüfungen. Dieser umfassende Ansatz ermöglicht es uns, nicht nur externe Bedrohungen zu identifizieren, sondern auch Schwachstellen innerhalb der IT-Infrastruktur aufzudecken. Durch die Berücksichtigung beider Perspektiven bieten wir eine ganzheitlichere Bewertung der Sicherheitslage eines Unternehmens und ermöglichen so eine gezieltere und effektivere Verbesserung der Cyberabwehrmaßnahmen.

4 Inventarisierung und Erkennung

In der Phase der Inventarisierung und Erkennung der ITK-Vektoranalyse erfolgt zudem eine detaillierte Bestandsaufnahme sämtlicher Hardware- und Softwarekomponenten innerhalb der IT-Infrastruktur eines Unternehmens. Dieser Schritt ist entscheidend, um einen umfassenden Überblick über die potenziell angreifbaren IT-Ressourcen zu gewinnen und bildet die Grundlage für die anschließende Analyse von Sicherheitslücken und Schwachstellen. Durch diese gründliche Erfassung können Unternehmen nicht nur ihre gegenwärtige Sicherheitslage besser verstehen, sondern auch effektiver planen, wie sie ihre Systeme vor zukünftigen Bedrohungen schützen können.

5 Sicherheitslücken aufdecken

Im Rahmen der ITK-Vektoranalyse spielt die Identifizierung und Priorisierung von Sicherheitslücken eine zentrale Rolle. Mithilfe fortschrittlicher Scanning-Technologien und Analyseverfahren werden Schwachstellen in der IT-Infrastruktur präzise erkannt. Diese Sicherheitslücken werden anschließend basierend auf ihrem potenziellen Risiko für das Unternehmen priorisiert. Dieser Prozess ermöglicht es, kritische Sicherheitsrisiken vorrangig anzugehen und eine effiziente Ressourcenallokation für die Behebung von Schwachstellen sicherzustellen, wodurch das Sicherheitsniveau signifikant erhöht wird.

6 Einhaltung von BSI-Vorgaben (KRITIS/NIS 2.0)

Die Einhaltung der BSI-Vorgaben durch die ITK-Vektoranalyse ist nicht nur für die Sicherheit von essenzieller Bedeutung, sondern auch für die Compliance und die Einhaltung gesetzlicher Vorgaben entscheidend! Unternehmen müssen eine Vielzahl rechtlicher Rahmenbedingungen beachten, da deren Nichtbeachtung zu erheblichen Strafen führen kann. Zudem birgt die Vernachlässigung der Cybersicherheit für Entscheidungsträger das Risiko der persönlichen Haftung. Die Analyse trägt dazu bei, diese Risiken zu minimieren, indem sie sicherstellt, dass die IT-Infrastruktur den aktuellen Sicherheitsstandards entspricht und gesetzliche Anforderungen erfüllt.

7 Nutzen und Vorteile der ITK-Vektoranalyse

Die ITK-Vektoranalyse bietet Unternehmen zahlreiche Vorteile: Sie ermöglicht eine umfassende Einsicht in die IT-Sicherheitslage durch eine Kombination von internen und externen Analysen. Dadurch wird eine ganzheitliche Risikoerkennung und -minderung gefördert. Die präzise Inventarisierung von Hardware und Software unterstützt die Compliance mit gesetzlichen Vorgaben und minimiert das Haftungsrisiko des Unternehmens und seiner Entscheidungsträger. Ebenso fördern die Ergebnisse die Abschlusswahrscheinlichkeit und Wirtschaftlichkeit von Cyber-Security Versicherungen.
Durch die Priorisierung von Sicherheitslücken können Ressourcen zudem effektiver zugewiesen werden, um die kritischsten Schwachstellen zuerst anzugehen. Hierdurch wird die Sicherheit und Resilienz des Unternehmens schrittweise und zielgerichtet signifikant verbessert.

8 Implementierung und Ablauf

Die Implementierung der ITK-Vektoranalyse beginnt mit einer anfänglichen Konsultation, um die spezifischen Bedürfnisse und Ziele des Unternehmens zu verstehen. Daraufhin folgt eine gründliche Inventarisierung der IT-Infrastruktur, gefolgt von internen und externen Sicherheitsprüfungen. Auf Grundlage der Ergebnisse werden Sicherheitslücken identifiziert und priorisiert. Abschließend werden Maßnahmenpläne entwickelt, um die identifizierten Schwachstellen effektiv anzugehen und die Einhaltung der BSI-Vorgaben sicherzustellen.

Umsetzung der N I S 2 – Direktive

1 Sicherheitsziele erfüllen mit ITK Ingenieure Service GmbH

Die NIS-2-Richtlinie ist eine neue EU-weite Verfassung über die neuen Richtlinien der Netzwerk- und Informationssicherheit, die von allen betroffenen Unternehmen bis zum 17. Oktober 2024 umgesetzt werden muss. Durch die neue Richtlinie steigt die Anzahl der betroffenen Unternehmen erheblich. Betroffene Unternehmen müssen Ihre IT-Sicherheitsmaßnahmen prüfen und ggf. an den neuen Standard anpassen.

Ob ein Unternehmen betroffen ist oder nicht, muss es selbst anhand der neuen NIS2-Kritieren einschätzen und bewerten.

Konkrete technische Maßnahmen gibt die NIS2-Richtlinie allerdings nicht vor. Sie verweist auf Branchenstandards wie B3S. Es gibt generell eine große Überlappung mit der ISO/IEC 27001.

Aus der NIS2-Directive lassen sich jedoch grundlegende Sicherheitsziele ableiten. ITK Ingenieure Service GmbH und Partner unterstützen Sie bei der Umsetzung und kontinuierlichen Einhaltung dieser Ziele aus den NIS2-Anforderungen.

Risikoanalyse und Sicherheit für Informationssysteme

- Verfahren zur regelmäßigen Risikoanalyse und Schwachstellenbewertung einführen
- Asset Discovery, Beschreibung und Softwareinventarisierung
- Bestehende Schwachstellen und Sicherheitslücken identifizieren
- Regelmäßige Penetrationstest der eigenen Infrastruktur und bisher ergriffen Sicherheitsmaßnahmen
- ISMS nach ISO 27001, TISAX, etc. umsetzen

Bewältigen von Sicherheitsvorfällen

- End-to-end Anomalie- und Angriffserkennung ermitteln. Protokollierung aller Ereignisse und Ableitung automatischer Reaktionen. **
- Angriffe, böswillige, fehlerhafte oder andere Aktivitäten im Netz, die sich auf kritische Dienste auswirken könnten, frühzeitig zu erkennen
- Schnelle Reaktion auf Cybervorfälle sicherstellen (Incident Response) ermöglichen
- Schadsoftware und Angreifende an Netzwerkgrenzen bestmöglich abwehren
- Managed Detection and Response Services

Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisenmanagement

- Störung der Prozesse durch Sicherheitsmaßnahmen vermeiden
- Business-Continuity-Plan erstellen
- Mehrstufiges Backup-Management etablieren
- Schnelle Notfallwiederherstellung ermöglichen
- Professionelle Krisenbewältigung und -kommunikation einrichten

Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit

- Die technische Kommunikation der Schnittstellen überwachen, auswerten und ggf. automatisierte Maßnahmen etablieren.
- Least Privilege Access für Lieferanten etablieren
- Sicheren Lieferanten-Zugang zum Netzwerk gewährleisten (z. B. sichere Passwörter, VPN)

Sicherheit in der Entwicklung, Beschaffung und Wartung, Management von Schwachstellen

- Regelmäßige Penetrationstest eigener Software und Infrastruktur
- Dauerhaftes Monitoring von Schwachstellen
- Effektive und sichere Behandlung und von Schwachstellen sicherstellen

7 Bewertung der Effektivität von Cybersicherheit und Risikomanagement

- Die Wirksamkeit des Cybersicherheit-Systems fortlaufend überprüfen und verbessern mit Hilfe von automatisierten Pentests
- Cybersicherheitslage und Risikoexposition regelmäßig neu bewerten

8 Schulungen Cybersicherheit und -Hygiene

- Defense-in-Depth-Architektur aufbauen, um Versagen der Perimetersicherung frühzeitig zu erkennen und interne Netzwerk Kommunikation Umfang zu überwachen
- Gefährdete Assets überwachen und abschirmen, bei denen Patches/Aktualisierungen nicht möglich sind
- Ausbreitung von Angriffen eindämmen (z. B. durch Netzsegmentierung)
- Digitale Ressourcen in Bezug auf Firmware, Betriebssystem usw. auf dem neusten Stand halten
- Starke Passwortrichtlinien festlegen und umsetzen
- Regelmäßige Cybersicherheitsschulungen für das Personal umsetzen

9 Kryptografie und Verschlüsselung

- Überwachung und Überprüfung verschlüsselter Verbindungen nach aktuellem Stand der Technik. Abgleich TLS nach TR-03116-4 Checkliste des BSI
- Einrichtung und Sicherstellung einer durchgehenden verschlüsselten Kommunikation im internen Netz

10 Personalsicherheit, Zugriffs- Kontrolle und Anlagenmanagement

- Zugriffe auf kritische Dateien und Verzeichnisse Unternehmensweit überwachen.
- Sicherheitsüberprüfungen und -sensibilisierung in das Einstellungs- und Vertragsvergabeverfahren integrieren
- Unbefugten physischen Zugriff auf Assets verhindern

11 Sichere Kommunikation (Sprach, Video- und Text)

- Überwachung sämtlicher Kommunikationssysteme und der Verschlüsselten Verbindungen
- Innerhalb von 24 Stunden nach einem Vorfall Frühwarnung an CSIRT*** übermitteln
- Innerhalb von 72 Stunden erste Bewertung an CSIRT übermitteln (inkl. Aussagen zu Schweregrad, Auswirkungen, Quelle)
- Auf Anfrage des CSIRT Aktualisierungen zum Status des Vorfalls Managements bereitstellen
- Innerhalb eines Monats detaillierten Berichts an das CSIRT übermitteln (inkl. Informationen zu Schweregrad, interne und grenzüberschreitende Auswirkungen, Ursache, Abhilfemaßnahmen)

12 Multi-Faktor Authentisierung und kontinuierliche Authentisierung

- Unbefugten Zugriff auf digitale Assets verhindern. Überwachung aller Logins und Loginversuche
- Personalisierte Multi-Faktor-Authentifizierung sicherstellen
- Sichere digitale Kommunikation gewährleisten

* Die aufgeführten Ziele sind in der NIS2 nicht explizit definiert, sondern spiegeln allgemeine grundlegende Sicherheitsziele wider, wie sie in internationalen Normen wie der IEC 62443 empfohlen werden.
** Verpflichtend für kritische Infrastrukturen. Umsetzung erfolgt durch separaten Auftrag
*** CSIRT (Computer security incident response team) = behördliches Computer-Notfallteam

Kontakt und Beratung

Hans Oberlechner
Senior Consultant
Tel: 0 20 54 | 1 69 79 - 0
Mobil: 01 51 | 17 43 02 70
Mail: hans.oberlechner@itk-ingenieure.de

Kai Dietrich
Bereichsleiter
Tel: 0 20 54 | 1 69 79 – 0
Mobil: 01 73 | 28 19 932
Mail: kai.dietrich@itk-ingenieure.de

Richard Logan
Senior Consultant
Tel: 0 20 54 | 1 69 79 – 0
Mobil: 01 72 | 98 90 283
Mail: richard.logan@itk-ingenieure.de