RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Cyberschutz
Rheinland-Pfalz

Spionage und Sabotage

Guido Jost
Cybersicherheit-Wirtschaftsschutz
Ministerium des Innern und für Sport

© Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau Rheinland-Pfalz

Die fortschreitende Digitalisierung hat die IT zur Lebensader von Unternehmen gemacht.

Fallen Anwendungen aus oder ist der Zugriff auf Daten eingeschränkt, können Mitarbeiter ihre Aufgaben nicht mehr erledigen und Geschäftsprozesse stehen still.

Die Ursachen für solche Unterbrechungen sind vielfältig.

Insbesondere Supply-Chain-Attacken, also Angriffe auf die Lieferkette, bergen ein hohes Schadenspotential.

Cyber Resilience Act der EU

Der Cyber Resilience Act bringt „Security-by-Design“.

Im September 2022 hat die Europäische Kommission einen ersten Entwurf für den Cyber Resilience Act (CRA) vorgelegt.

Der Entwurf soll die digitale Sicherheit durch gemeinsame Cyber-Sicherheitsstandards für vernetzte Geräte und Dienste nachhaltig in Europa verankern.

NIS-2 Maßnahmen zur Cybersicherheit

Die NIS-2 Richtlinie ist die aktuelle EU-weite Gesetzgebung, um die allgemeine Cybersicherheit in der Europäischen Union zu erhöhen.

Unternehmen müssen abhängig von Sektor und Größe bestimmte Anforderungen an die Cybersicherheit erfüllen.

Dazu gehören unter anderem:

NIS-2 Maßnahmen zur Cybersicherheit

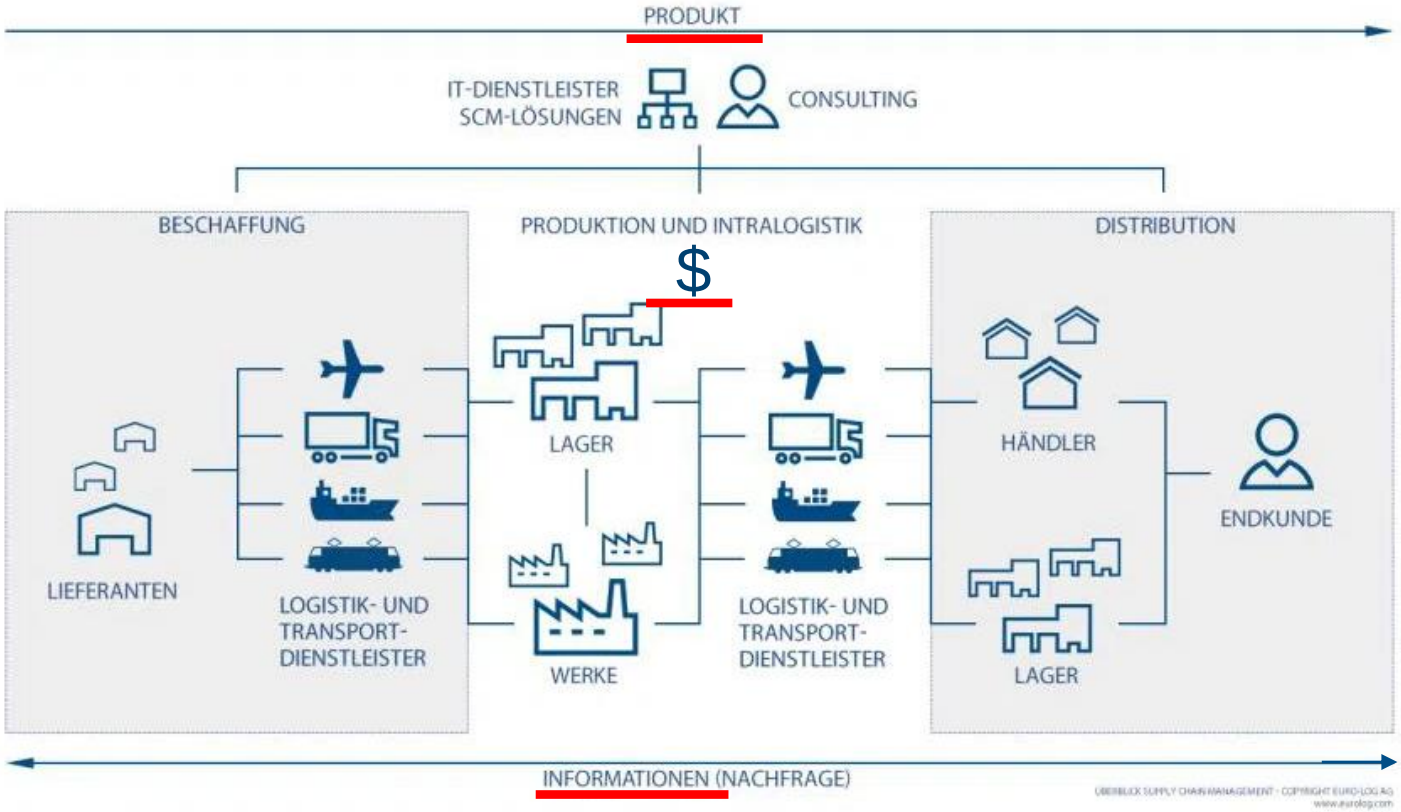
- Aufbau von Cybersicherheit nach einschlägigen internationalen Normen (z. B. ISO/IEC 27001)
- Die Durchführung regelmäßiger Risikobewertungen und Audits
- Die Meldung von Sicherheitsvorfällen an die zuständigen Behörden
- Regelmäßige Cyber-Trainings der Mitarbeiter
- Sicherstellung der Informationssicherheit in der Lieferkette.

Cyber-Angriffe auf digitale Lieferketten

Zur Supply-Chain gehören alle Zulieferer, Dienstleister und Kunden, mit denen ein Unternehmen weltweit zusammenarbeitet.

Dadurch ergibt sich eine Reihe von Problemen, die damit beginnen, dass diese Unternehmen sehr unterschiedliche Ziele, Interessen, Sicherheitsbedarfe und in Folge auch unterschiedliche Sicherheitsregeln (Policies) verfolgen!

Supply-Chain Komponenten



That‘s not my job!

Angriffe auf die Software-Lieferkette werden in der Regel dadurch ermöglicht, dass Hersteller die Sicherheit erst am Ende des Entwicklungsprozesses prüfen.

Ein bösartiger Code, der während der Entwicklung eingeschleust wurde, gilt als vertrauenswürdig, weil die endgültige Version am Ende des Prozesses abgenommen wird.

Gelingt es Angreifern den Quellcode der Produkte zu manipulieren, dann fehlt es vielen Unternehmen an der nötigen Transparenz und den notwendigen Schutzmaßnahmen.

Zombie-Sicherheitslücken

Dabei handelt es sich beispielsweise um alte Sicherheitslücken, die als längst gepatcht galten.

Diese tauchen dann in Programmen und eben auch Geräten wieder auf, weil alte, ungepatchte Software-Bibliotheken in neuen Projekten verwendet werden.

Wie können wir Sie unterstützen?

- Um sich vor Angreifern über die Lieferkette zu schützen, ist die kontinuierliche Überwachung (Management) des Supply-Chain-Prozesses unumgänglich.
- Neben der Implementierung **umfassender Cybersicherheit** durch **EDR-**, **MDR-** oder **Threat Intelligence-Technologien**, spielen die Einführung und Kommunikation entsprechender Richtlinien und **Mitarbeitersensibilisierung** eine entscheidende Rolle.

Cyber-Threat Intelligence

Unter dem Begriff Cyber-Threat Intelligence versteht man das Wissen über aktuelle und mögliche Bedrohungen, Angriffsszenarien und Schadprogramme.

Cyber-Threat Intelligence ist also keine Sicherheitssoftware, sondern eine Sammlung von Daten, die für die gezielte Abwehr potenzieller Angriffe genutzt werden kann.

Das Sicherheitsportal - Cyberschutz Rheinland-Pfalz:

bündelt Informationen zu Cyberangriffen und zu konkreten technischen Absicherungsmöglichkeiten zum Schutz vor Cyberspionage und Cybersabotage.

Das als Herzstück in einer cloud-basierten Lösung Bedrohungsindikatoren (IOC‘s) für die Organisationen kostenlos zum Download bereitstellt.

Cyberschutz
Rheinland-Pfalz

RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Cyberschutz Rheinland-Pfalz

Der Verfassungsschutz Rheinland-Pfalz unterstützt die Cyber- und IT-Sicherheit rheinland-pfälzischer Unternehmen ab sofort mit einem neuen Angebot. Das Sicherheitsportal Cyberschutz Rheinland-Pfalz bündelt Informationen zu Cyberangriffen und zu konkreten technischen Absicherungsmöglichkeiten zum Schutz vor Cyberspionage und Cybersabotage. Das Angebot richtet sich insbesondere an kommunale Unternehmen der kritischen Infrastruktur. Weitere Informationen dazu in der Pressemeldung.

Schutz vor Cyberangriffen im Video erklärt

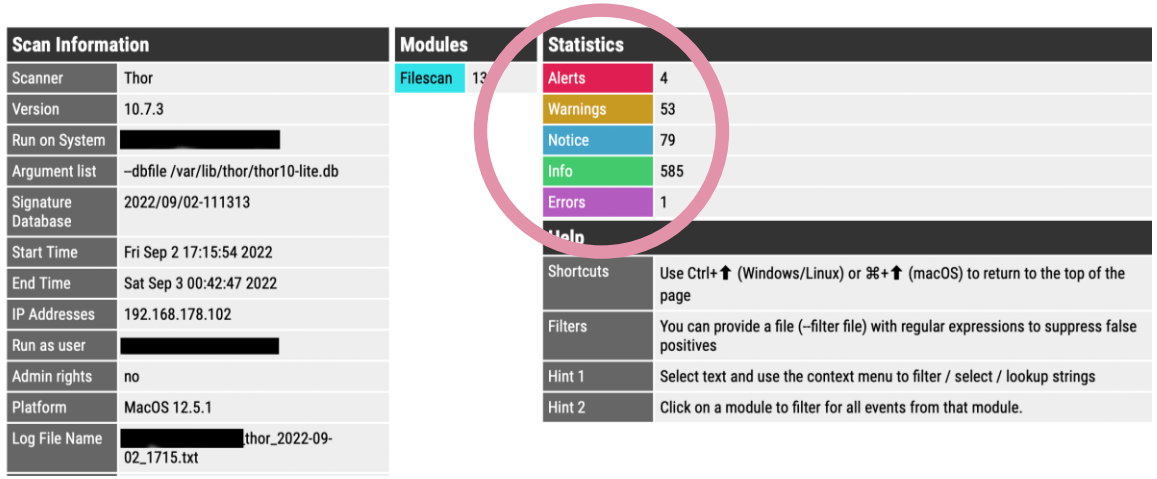
Kontakt

Cyberschutz
Rheinland-Pfalz

Haben Sie Fragen zum Cyberschutz Rheinland-Pfalz?

Sie erreichen den Cyberschutz per E-Mail an cyberschutz(at)mdi.rlp.de.

Für einen Zugang benötigen wir eine Funktionsadresse ohne personenbezogenen Daten wie zum Beispiel it@ihrefirma.de.



Scan Information	
Scanner	Thor
Version	10.7.3
Run on System	[redacted]
Argument list	--dbfile /var/lib/thor/thor10-lite.db
Signature Database	2022/09/02-111313
Start Time	Fri Sep 2 17:15:54 2022
End Time	Sat Sep 3 00:42:47 2022
IP Addresses	192.168.178.102
Run as user	[redacted]
Admin rights	no
Platform	MacOS 12.5.1
Log File Name	[redacted]thor_2022-09-02_1715.txt

Modules	
Filescan	13

Statistics	
Alerts	4
Warnings	53
Notice	79
Info	585
Errors	1

Help	
Shortcuts	Use Ctrl+⬆ (Windows/Linux) or ⌘+⬆ (macOS) to return to the top of the page
Filters	You can provide a file (--filter file) with regular expressions to suppress false positives
Hint 1	Select text and use the context menu to filter / select / lookup strings
Hint 2	Click on a module to filter for all events from that module.

Alerts

Alert 1

Sep 2 22:39:24 [redacted] 192.168.178.102

MODULE: Filescan
MESSAGE: Malware file found
FILE: /System/Volumes/Data/Volumes/[redacted]ibraries/org/apache/logging/log4j/log4j-core/2.0-beta9/log4j-core-2.0-beta9.jar
EXT: .jar
SCORE: 100
TYPE: ZIP
SIZE: 681134
MD5: 152ecb3ce094ac5bc9ea39d6122e2814
SHA1: 678861ba1b2e1fccb594bb0ca03114bb05da9695
SHA256: dcde6033b205433d6e9855c93740f798951fa3a3f252035a768d9f356fde806d
FIRSTBYTES: 504b03040a0000000000923a2e43000000000000 / PK :.C
CREATED: Mon Dec 30 01:14:26.000 2019
CHANGED: Wed Feb 23 21:01:12.000 2022
MODIFIED: Sun Jan 5 19:01:56.000 2014
ACCESSED: Wed Feb 23 21:01:12.000 2022
PERMISSIONS: -rwx------
OWNER: [redacted]
GROUP: staff

REASON_1: Vulnerable Log4j library ./apache-log4j-2.0-beta9-bin/log4j-core-2.0-beta9.jar
SUBSCORE_1: 100
REF_1: SHA256 hash list
SIGTYPE_1: internal
MATCHED_1:

Alert 2

Sep 2 22:39:24 [redacted] 192.168.178.102

Im Scan-Report zeigt Thor seine Funde: Bedrohungen (Alerts) und Warnungen (Warnings) sollten Sie umgehend prüfen und Maßnahmen einleiten.

Cyberschutz
Rheinland-Pfalz

RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Der Cyberschutz Rheinland-Pfalz ist unter

www.cyberschutz.rlp.de

aufrufbar.

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Vielen Dank für Ihre Aufmerksamkeit

Guido Jost
IT-Geheimschutzverantwortlicher

Ministerium des Innern und für Sport

cyberschutz@mdi.rlp.de