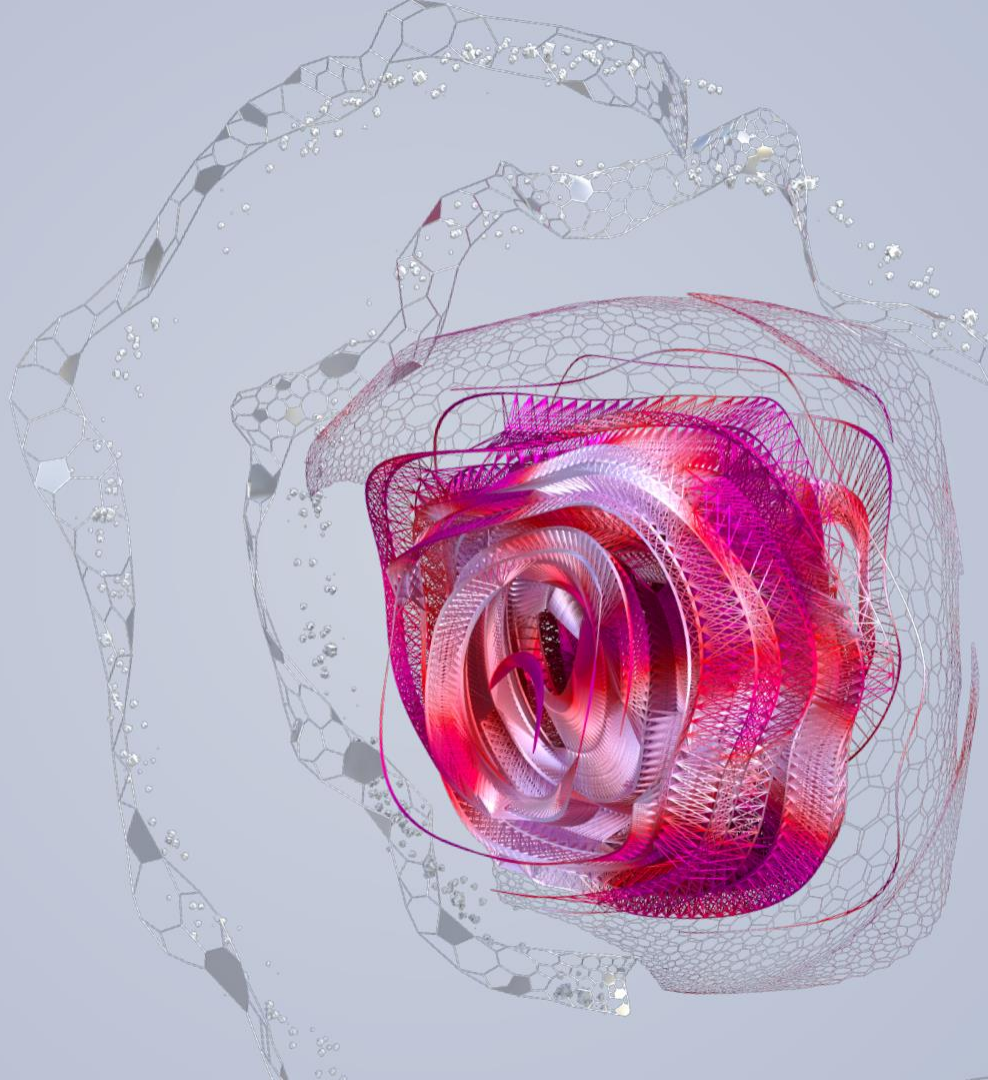
Warum sind Cyberangriffe erfolgreich

Richard Werner, Business Consultant



Ursachen – nach Kategorie

- Mangelnde/Fehlende Prozesse
- Technische Schwachstellen
- Menschliche “Fehler”

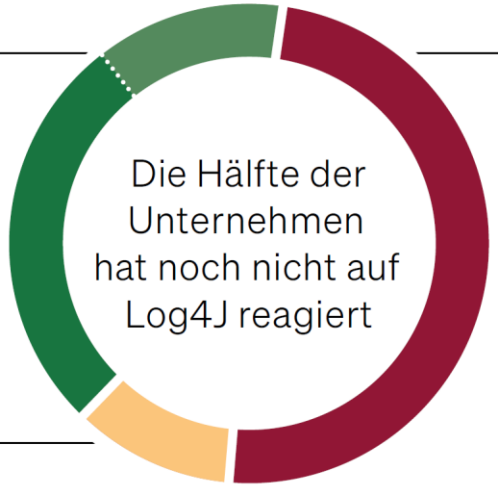
Prozesse

Log4J: Alarmstufe ROT – aber vielerorts keine Reaktion

Anteil der Unternehmen, die ihre Software und Systeme
nach Bekanntwerden der Sicherheitslücke „Log4J“ überprüft haben

40 %
haben ihre **Software** auf die Log4J-Schwachstelle überprüft; davon haben nur zwei Drittel ihre **Systeme** auf bereits eingedrungene Schadsoftware geprüft

11 %
machen dazu keine Angaben



49 %
haben weder **Software** noch **IT-System** geprüft

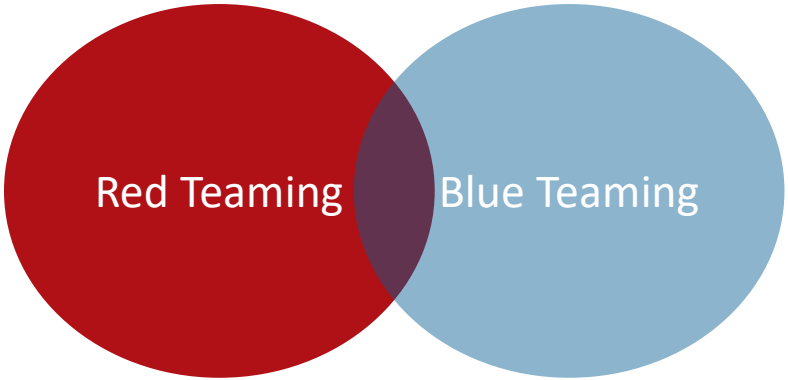
Wie schnell können Sie Security News verarbeiten?

Quelle: Forsa-Befragung von 300 mittelständischen Unternehmen, April/Mai 2022

GDV Gesamtverband der Versicherer

Notfall und Backup Handling

- Wie aktuell sind die Prozesse?
- Sind die Schritte erprobt?
- Verantwortungen und “Zugang” zu den Prozessen



Purple Teaming

Technische Schwachstellen

Von aussen angreifbar

Exchange Server RCE Vulnerability – Ausnutzung laut Microsoft “unwahrscheinlich”

Ebenfalls Exchange Server RCE – Wird bereits in Angriffen verwendet

CERT.at

Meldungen Services Downloads Über uns Berichte

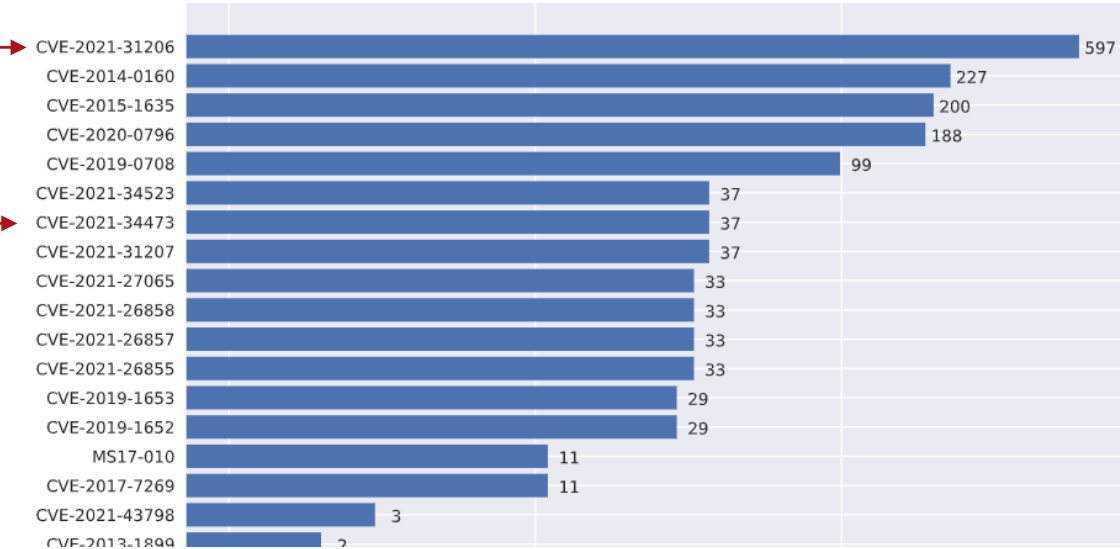
› Meldungen › Aktuelles › Show

Warnungen **Aktuelles** Tagesberichte Blog Spezielles

09.08.2022 11:31

Shodan Verified Vulns 2022-08-01

Mit Stand 2022-08-01 sieht Shodan in Österreich die folgenden Schwachstellen:



Von Tätern ausgenutzte Software Schwachstellen

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

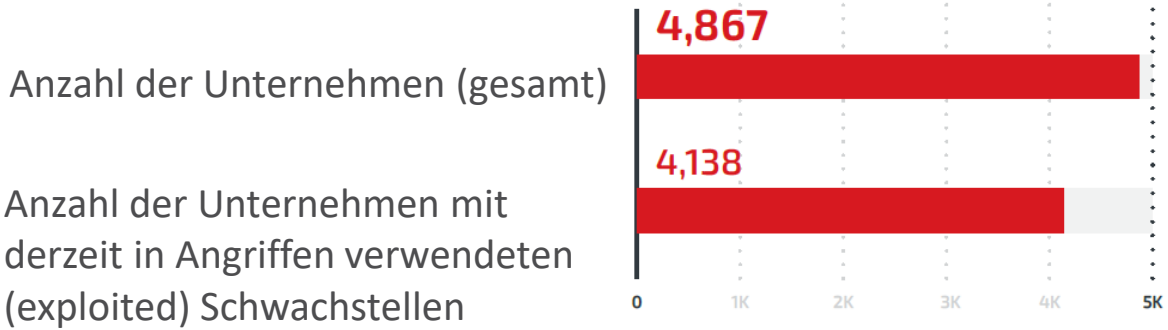
Datenbank initiiert:
November 2021

Stand 06.09.2022:

Erfasste Schwachstellen: 812
Davon Hersteller Microsoft: 239

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action
CVE-2022-26352	dotCMS	dotCMS	dotCMS Unrestricted Upload of File Vulnerability	2022-08-25	dotCMS ContentResource API contains an unrestricted upload of file with a dangerous type vulnerability that allows for directory traversal, in which the file is saved outside of the intended storage location. Exploitation allows for remote code execution.	Apply updates per vendor instructions.
Notes	https://www.dotcms.com/security/SI-62					
CVE-2022-24706	Apache	CouchDB	Apache CouchDB Insecure Default Initialization of Resource Vulnerability	2022-08-25	Apache CouchDB contains an insecure default initialization of resource vulnerability which can allow an attacker to escalate to administrative privileges.	Apply updates per vendor instructions.
Notes	https://lists.apache.org/thread/w24wo0h8nlctfps65txvk0oc5hdcnv00					
CVE-2022-24112	Apache	APISIX	Apache APISIX Authentication Bypass Vulnerability	2022-08-25	Apache APISIX contains an authentication bypass vulnerability that allows for remote code execution.	Apply updates per vendor instructions.
Notes	https://lists.apache.org/thread/lcdqywz8zy94mdysk7p3gfdgn51jmt94					
CVE-2022-22963	VMware Tanzu	Spring Cloud	VMware Tanzu Spring Cloud Function Remote Code Execution Vulnerability	2022-08-25	When using routing functionality in VMware Tanzu's Spring Cloud Function, it is possible for a user to provide a specially crafted SpEL as a routing-expression that may result in remote code execution and access to local resources.	Apply updates per vendor instructions.

Verwundbarkeit in Unternehmen



Quelle: Trend Micro – Risikoanalyse-Kunden Weltweit August 2022

Schwachstellen intern

Von Angreifern bevorzugte Schwachstellen hinter der Perimeterverteidigung

Januar – Juni 2022

Quelle: Trend Micro Kunden weltweit

Filter ID	Solution	Related CVEs	Detected event counts
1009667	Deep Security	CVE-2017-14495	114,995,958,044
1000853	Deep Security	CVE-2006-4154	5,665,473,527
1011242	Deep Security	CVE-2021-44228	4,794,466,414
1003766	Apex One	CVE-2009-2524	995,700,958
1004398	Deep Security	CVE-2010-2730	967,669,441
1010971	Deep Security	CVE-2021-29441	846,824,548
1006027	Deep Security	CVE-2014-0098	417,996,287
1011456	Deep Security	CVE-2022-26134	381,361,877
1008445	Apex One	CVE-2017-8543	266,267,487
1008713	Apex One	CVE-2017-11815	188,900,588

Log4Shell

Menschliche “Fehler”

Noch(!) haben Sie gute Chancen durch Mitarbeiterschulungen

LAPSUS$ channel

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

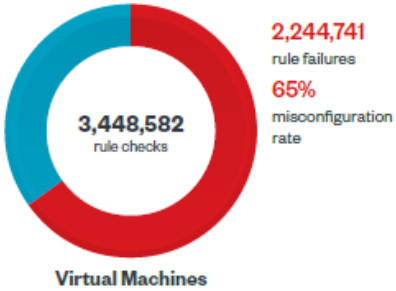
You will be paid if you would like. Contact us to discuss that

@lapsusjobs 624 13.3K 12:37 PM

“MFA – Fatigue” Angriffe

Fehlkonfiguration & Fehleinschätzung

AWS



Azur

Gründe für Fehlkonfigurationen:

- Unkenntnis
- Zeitnot
- Mangelnde Dokumentation
- Absicht/Workaround
- Missverständnisse
- „Schatten – IT“

Quelle: Trend Micro Cloud One Conformity – 2021
Top Misconfigured Services AWS & Azur

Die Herausforderung der Zukunft

Das eigene Risiko einschätzen

Priorisierung von Aufgaben
Akzeptanz von Lücken

Abhängigkeit von IT

Fehlende/veraltete Dokumentation

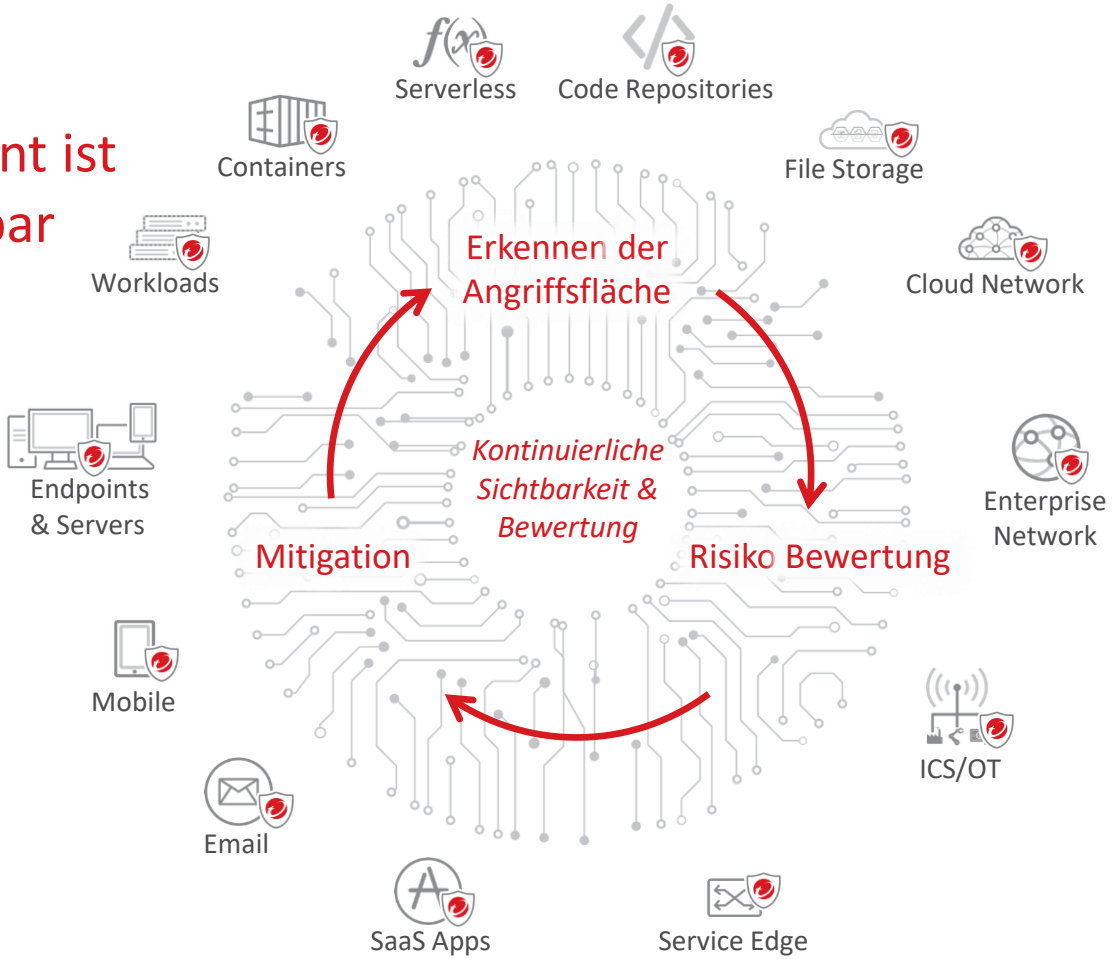
Schnelle Bereitstellung
Konstante Verfügbarkeit

Nutzerverhalten & -kenntnisse

Inkompatibilitäten
Veraltete Systeme

Überarbeitete IT(-Security)
Fachkräftemangel

IT-Risiko Management ist unverzichtbar



TREND MICRO™

THE ART OF CYBERSECURITY

Extended detection and response across multiple IT layers by Trend Micro. **Created with real data by artist Brendan Dawes.**