SOCRadar®
Your Eyes Beyond

Bericht zur Cyber-Bedrohungslandschaft in Deutschland 2023

socradar.io

Inhaltsverzeichnis

Zusammenfassung

Deutschland ist nach den Vereinigten Staaten, China und Japan die viertgrößte Volkswirtschaft der Welt und die größte in Europa. Außerdem ist es der drittgrößte Exporteur der Welt. Obwohl das Land für seine Schwerindustrie und das verarbeitende Gewerbe bekannt ist, trägt die Dienstleistungsbranche mit 70 % am meisten zum BIP (Bruttoinlandsprodukt) bei. Darüber hinaus spielt Deutschland eine wichtige Rolle in der europäischen Politik und war Ziel verschiedener Angriffe, darunter auch Cyberspionage, durch unterschiedliche Bedrohungsakteure. Organisationen sowohl im öffentlichen als auch im privaten Sektor, insbesondere solche, die an geopolitisch bedeutsamen Projekten beteiligt sind, sind nach wie vor wichtige Ziele für solche Angriffe.

Spannungen wie die Russland-Ukraine-Krise haben zu einer Zunahme von Cyberangriffen auf Länder geführt, die in Opposition zu Russland stehen. Laut einem von Thales im März 2023 veröffentlichten Bericht zur Analyse von Cyberbedrohungen stieg der Anteil der Cyberangriffe auf Länder der Europäischen Union (EU) in den sechs Monaten nach Ausbruch der Russland-Ukraine-Krise von 9,8 % auf 46,5 %. Dieser Anstieg steht in direktem Zusammenhang mit dem Konflikt; 61 % der im Laufe eines Jahres weltweit registrierten Angriffe gingen von Russland aus und richteten sich hauptsächlich gegen Länder, die Kiew unterstützen.

Diese Bedrohungen stellen auch für deutsche Organisationen ein erhebliches Risiko dar. Deutschlands technologischer Fortschritt, seine Wirtschaftskraft und seine zentrale Rolle in der europäischen und globalen Politik machen es zu einem attraktiven Ziel für staatlich gesponserte Cyberangreifer, die als Advanced Persistent Threats (APTs) bekannt sind, sowie für finanziell motivierte Angreifergruppen aus Ländern wie Russland, China und Iran.

Als Cyber Threat Actor versteht man eine Einzelperson oder eine Gruppe, die eine Bedrohung für die Cybersicherheit darstellt. Diese Akteure können vom Staat gesponsert werden oder als professionelle Einheiten agieren, die gemeinhin als APTs bezeichnet werden. Sie operieren in der Regel in der Anonymität, indem sie sich in versteckten Ecken des Internets aufhalten, die als "Dark Web" bekannt sind und von Suchmaschinen nicht indiziert werden. In diesen Dark-Web-Umgebungen, die oft als Underground bezeichnet werden, kommunizieren sie über Foren und Kanäle und tauschen und verkaufen eine Reihe von technischen Tools, Malware und Informationen, die sie aus Datenschutzverletzungen gewonnen haben. Dies unterstreicht die Bedeutung von Informationen über Cyber-Bedrohungen. Wenn Sie wissen, wem Ihre Daten gehören, können Sie Ihre Reaktionsmaßnahmen beeinflussen. Noch wichtiger ist es, Software-Schwachstellen zu erkennen, die von diesen Akteuren ausgenutzt werden. Die Gewinnung von Erkenntnissen über die Vorbereitungsphase der Cyberangreifer, ihre Profile und ihre Taktiken, Techniken und Verfahren (tactics, techniques, and procedures = TTPs) sind wesentliche Sicherheitsmaßnahmen.

SOCRadar kombiniert Open-Source- und Dark-Web-Informationen, um zuverlässige und umsetzbare Informationen zu liefern. Es warnt Sie vor potenziellen Cybervorfällen, die eskalieren könnten, und bietet Lösungen an. Die Sicherheitsanalysten von SOCRadar analysierten Daten von September 2022 bis September 2023, die durch die Überwachung von Untergrundforen und -kanälen, die von Bedrohungsakteuren rund um die Uhr genutzt werden, gesammelt wurden. Die Ergebnisse werden im Germany Threat Landscape Report 2023 vorgestellt. Der Bericht zielt darauf ab, Entscheidungsprozesse für Organisationen im öffentlichen und privaten Sektor zu unterstützen, indem er Einblicke in die Verwaltung und Reduzierung von Cybersicherheitsrisiken und die Verbesserung Ihrer Sicherheitslage bietet.

WICHTIGSTE ERKENNTNISSE

Die Sicherheitsanalysten von SOCRadar haben zwischen dem 1. September 2022 und dem 1. September 2023 mehr als 330 Dark-Web-Vorfälle (ohne Ransomware) im Zusammenhang mit Unternehmen mit Sitz in Deutschland entdeckt und analysiert. Sie kamen zu den folgenden wichtigen Schlussfolgerungen:

- Auf der Grundlage der über ein Jahr analysierten Daten sind die am stärksten von diesen Bedrohungen betroffenen Sektoren das Finanz- und Versicherungswesen, das kommerzielle Bankwesen, der elektronische Handel (insbesondere elektronische Einkaufs- und Versandhäuser), Informationsdienste, Telekommunikation, Einzelhandel und andere Sektoren.

- Die prominentesten Sektoren in der Kategorie "Andere Sektoren", die von Cybervorfällen betroffen sind, sind das Beherbergungsgewerbe, die Lebensmittelherstellung, das Transport- und Lagergeschäft sowie die Vermittlung von Rohstoffverträgen (einschließlich des Kryptowährungs- und NFT-Marktes).

- Mehr als 30 Sektoren und Teilsektoren wurden von diesen Cyber-Bedrohungen betroffen. Dies ist ein deutlicher Beweis dafür, dass sich die Angriffsfläche von Internetdiensten vergrößert, die Schwachstellen zunehmen und böswillige Akteure daraus Kapital schlagen, indem sie eine Strategie der sektoralen Expansion verfolgen.

- Innerhalb eines Jahres wurden 152 Ransomware-Angriffe von 26 verschiedenen Ransomware-Gruppen durchgeführt, die auf Organisationen in Deutschland abzielten. Gemessen an der Zahl der Opfer waren die erfolgreichsten Ransomware-Akteure LockBit 3.0 (mit 32 Opfern), BlackBasta (29), Cl0p (18), Play (12), Royal (12) und AlphVM Blackcat (11).

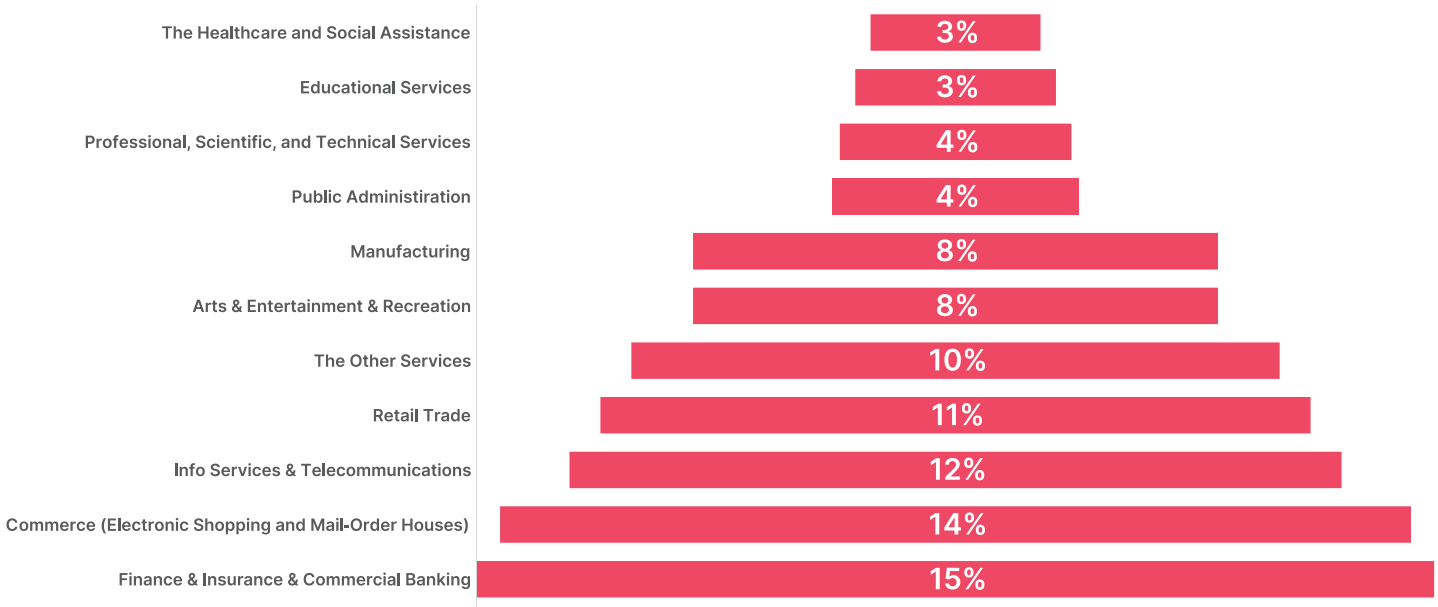
- Die nach der Anzahl der Vorfälle am stärksten von Ransomware-Angriffen bedrohten Branchen sind das verarbeitende Gewerbe (46 Vorfälle), freiberufliche-, wissenschaftliche- und technische Dienstleistungen (18), Informationsdienste (13) und der Einzelhandel (13).

- Nach den Beobachtungen von SOCRadar gehören zu den Advanced Persistent Threat (APT)-Gruppen, die es auf Organisationen in Deutschland abgesehen haben, Ice Fog, Turla Group, TA866 und Charming Kitten (auch bekannt als APT35). Killnet ist für seine DDoS-Angriffe auf NATO-Länder berüchtigt.

Spotlight auf: Bedrohungen aus dem Dark Web für die deutsche Industrie

Innerhalb des letzten Jahres wurden mehr als 330 Cyber-Vorfälle, zumeist Datenschutzverletzungen, aufgedeckt, die sich gegen Organisationen des privaten und öffentlichen Sektors in Deutschland richteten; die Verteilung dieser Vorfälle nach Branchen ist nachstehend aufgeführt. Mehr als 30 Sektoren und Untersektoren waren von diesen Cybervorfällen betroffen. Dies deutet auf die Vergrößerung der Angriffsflächen und die Verbreitungsstrategien der Bedrohungsakteure hin und zeigt somit deutlich, dass die Zahl der Opfer steigt.

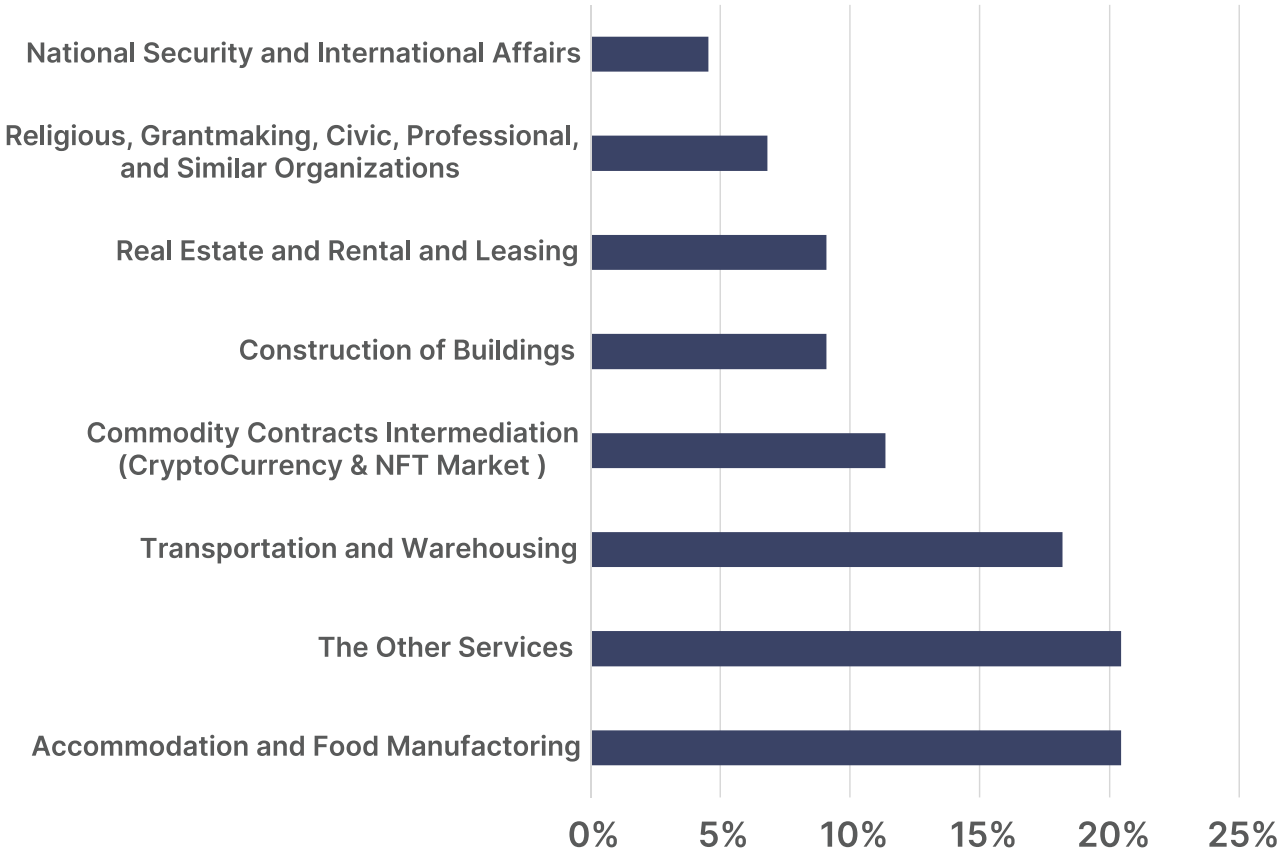
Verteilung der Cybervorfälle deutscher Organisationen, nach Branche



Spotlight auf: Bedrohungen aus dem Dark Web für die deutsche Industrie

Die Aufschlüsselung nach Branchen und Unterbranchen in der Kategorie "Sonstige Dienstleistungen", die 10 % des fünften Platzes unter den von den Bedrohungsakteuren ins Visier genommenen Branchen ausmacht, ist ebenfalls unten dargestellt. Wie im Verizon Data Breach Investigation Report dargelegt, wird die Bedeutung dieser exponierten Daten deutlich, wenn man bedenkt, dass bestätigte Datenschutzverletzungen etwa 10 % des tatsächlichen Prozentsatzes ausmachen. Ohne die Überwachung von Dark-Web-Foren und -Kanälen, bei denen die Maßnahmen gegen Cyber-Bedrohungen, die nur im "Clear Web" erkannt werden, nicht ausreichen, ist es nicht möglich, genau zu bestimmen, welche Art von Daten bei den einzelnen Unternehmen gefährdet ist.

Verteilung der Cyber-Vorfälle in der Kategorie Sonstige Dienstleistungen

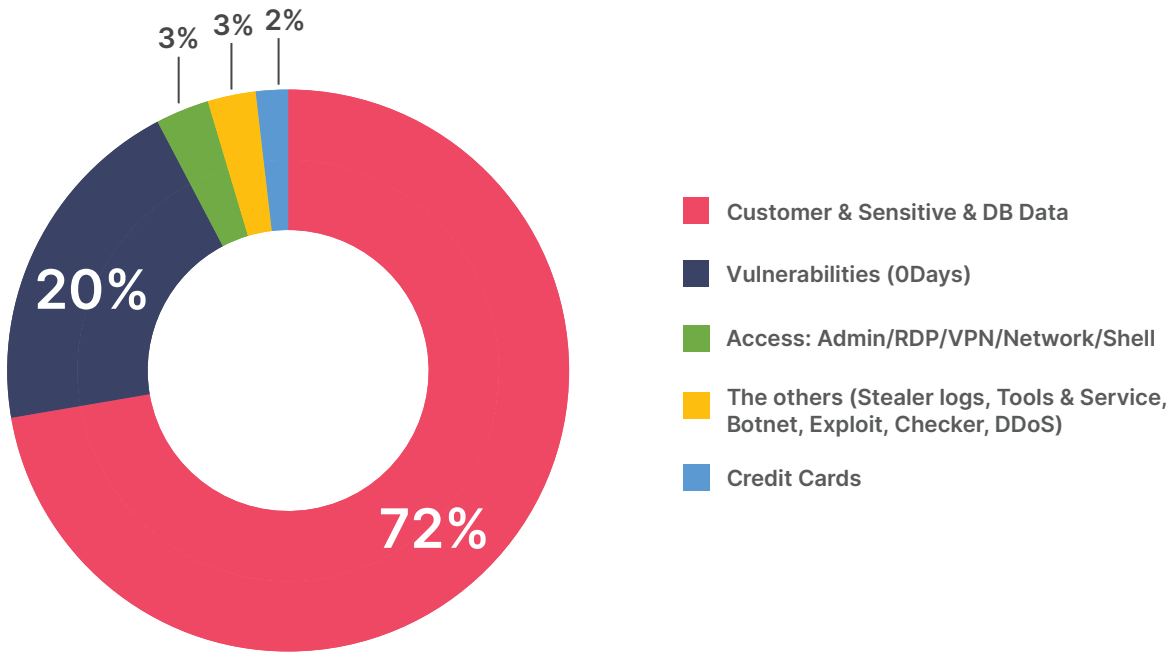


Spotlight auf: Bedrohungen aus dem Dark Web für die deutsche Industrie

Der unbefugte und illegale Zugriff auf persönliche Daten und Unternehmensdaten ist leider zu einem akzeptierten Risiko geworden, bei dem die Wahrscheinlichkeit eines Datenverlusts hoch ist. Laut einer Analyse von SOCRadar enthalten 72 % der verletzten Daten sensible Informationen wie Kundendaten. Informationen im Zusammenhang mit Admin-, RDP-, VPN-, Netzwerk- und Shell-Zugang, die für die ersten Phasen eines Cyberangriffs entscheidend sind, machen 20 % der angegriffenen Daten aus. Nach den Erkenntnissen der SOCRadar-Forschungsanalysten hat der Verkauf dieser Zugangsdaten deutlich zugenommen. Dies unterstreicht, dass die Aktivitäten im Dark Web nicht nur kompromittierte Daten umfassen, sondern auch wichtige Informationen, die für potenzielle zukünftige Cyberangriffe verkauft werden.

An fünfter Stelle, mit 2 % der Vorfälle, steht der Verkauf und die Weitergabe von Schwachstellen, die häufig von Cyberangreifern ausgenutzt werden, wie z. B. Zero-Day- und SQL-Injection-Schwachstellen. Wie der MOVEit-Vorfall zeigt, der seit Monaten für Aufregung sorgt, können Zero-Day-Schwachstellen, die in weit verbreiteter Software gefunden werden, eine Bedrohung für eine breite Palette von Unternehmen darstellen. Bis September 2023 waren über 1.100 Organisationen und mehr als 50 Millionen Menschen von der Ausnutzung der MOVEit-Schwachstellen durch die Cl0p-Ransomware-Gruppe, auch bekannt als TA505, betroffen. Derzeit sind 37 deutsche Organisationen von der MOVEit-Schwachstelle betroffen.

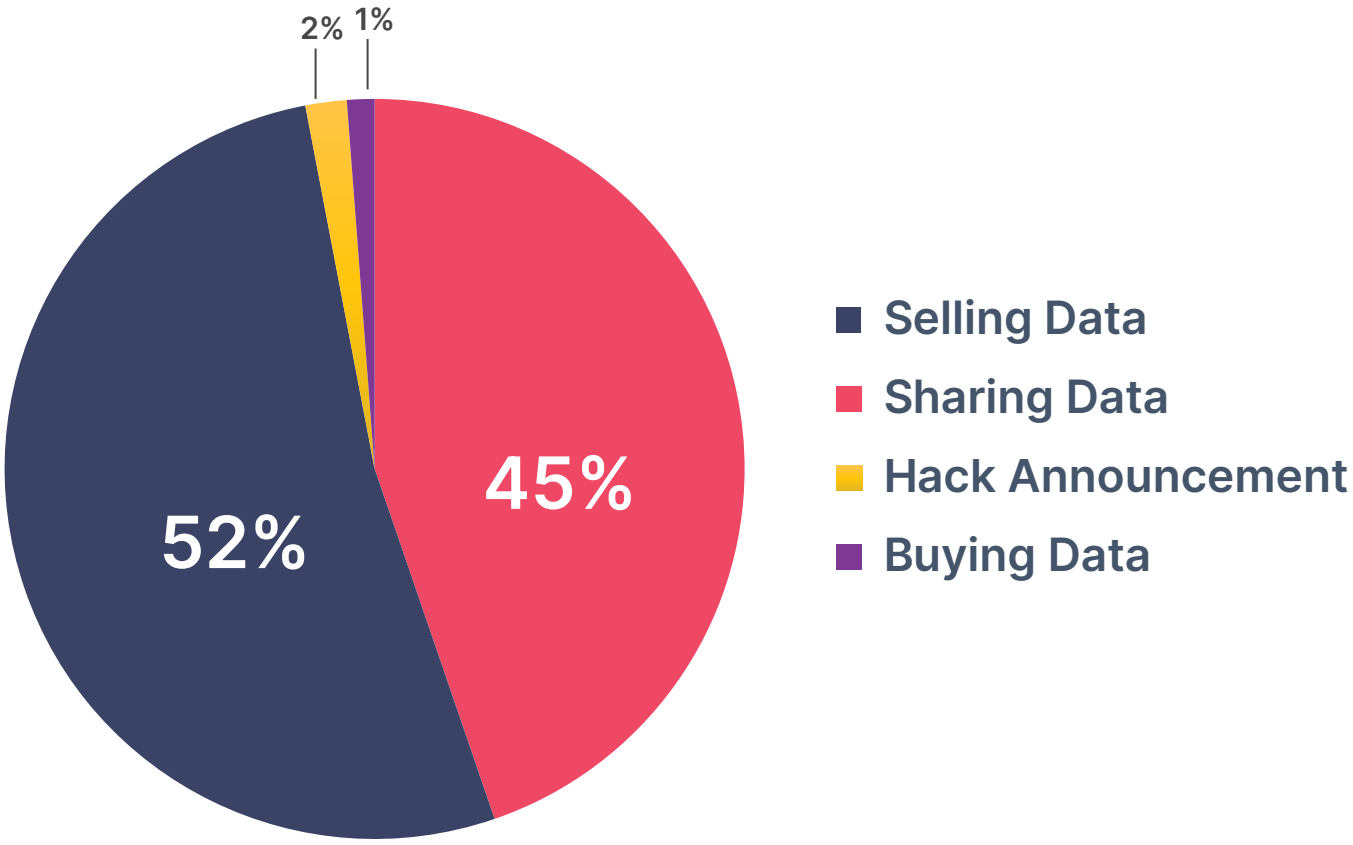
Verteilung nach Dark-Web-Post-Typen



Spotlight auf: Bedrohungen aus dem Dark Web für die deutsche Industrie

Im Folgenden wird die Verteilung der Daten in Dark-Web-Beiträgen nach der Art der Offenlegung dargestellt. Die Tatsache, dass mehr als die Hälfte der Beiträge (52 %) den Verkauf von Daten beinhalten, deutet auf einen Trend unter den Cyberangreifern hin, Daten nicht nur zu teilen, sondern sie auch schnell zu Geld zu machen.

Verteilung der Daten nach Offenlegungsarten

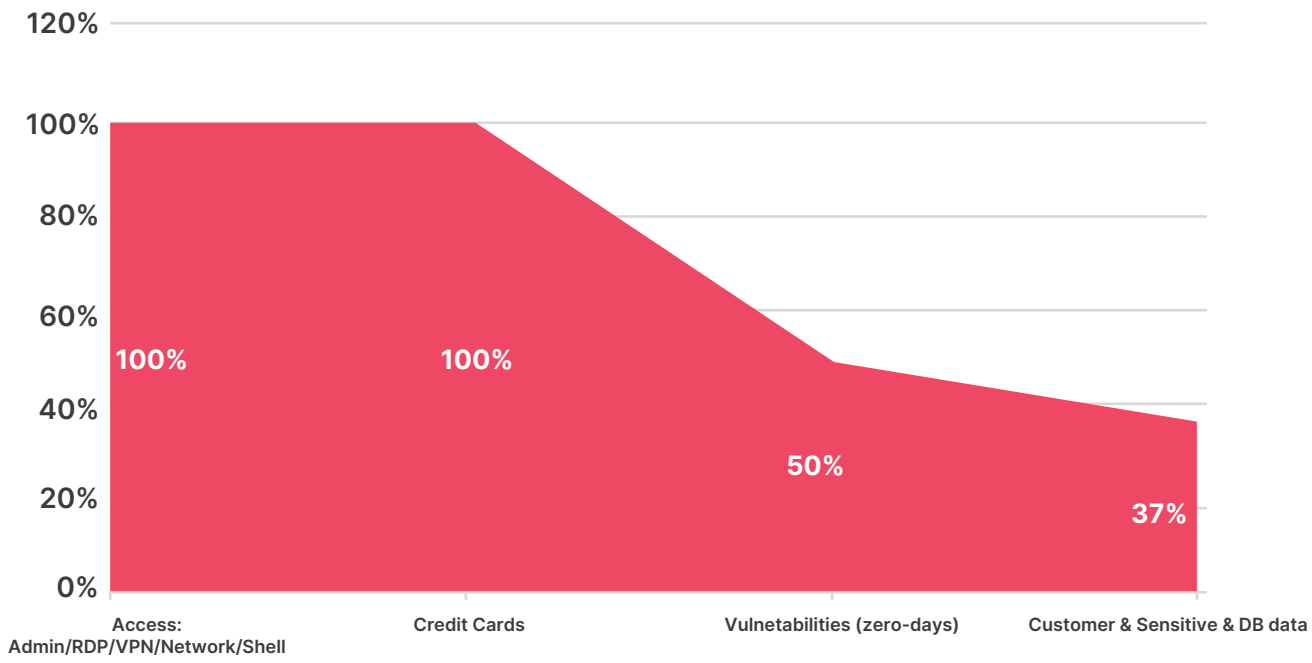


Spotlight auf: Bedrohungen aus dem Dark Web für die deutsche Industrie

Darüber hinaus handelt es sich bei der Mehrzahl der veröffentlichten Daten um persönliche, geschäftliche und sensible Informationen, die aus erfolgreichen Angriffen stammen. Dazu gehören auch Daten von Unternehmen, die kein Lösegeld gezahlt haben - eine Taktik, die als Double Extortion bekannt ist und von der Ransomware-Gruppen in letzter Zeit zunehmend Gebrauch gemacht haben.

Die proportionale Verteilung der zum Verkauf angebotenen Datentypen ist ebenfalls unten aufgeführt. Es wurde festgestellt, dass alle Zugangs- und Kreditkarteninformationen (100 %), die Hälfte der Sicherheitslücken wie Zero-Days (50 %) und 37 % der Daten mit persönlichen und sensiblen Informationen zum Verkauf angeboten wurden.

Prozentuale Verteilung der verkauften Daten nach Art



Jüngste Aktivitäten im Dark Web, die auf Einrichtungen in Deutschland abzielen

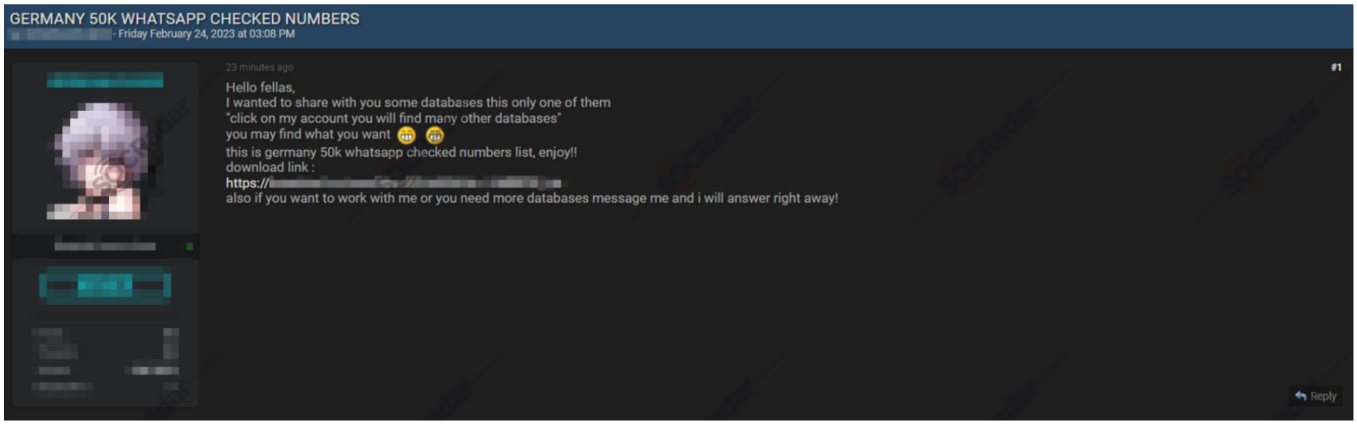
Im Jahr 2023 entdeckte und identifizierte das Dark-Web-Team von SOCRadar einige der bekanntesten Cybercrime-Aktivitäten im Dark Web, die auf deutsche Unternehmen abzielten. Diese Vorfälle werden in chronologischer Reihenfolge beschrieben, basierend auf der Art der in Untergrundforen gefundenen Postings.

Kunden- & Sensible & DB-Daten

Am 19. Januar 2023 wurde in einem von SOCRadar überwachten Hackerforum ein neues Datenleck für das German Institute for Global and Area Studies (www.giga-hamburg.de) entdeckt. Das GIGA ist ein deutsches Forschungsinstitut, das die politischen, wirtschaftlichen und sozialen Entwicklungen in Afrika, Asien, Lateinamerika und dem Nahen Osten analysiert. Außerdem betreibt es vergleichende Forschung zu internationalen Beziehungen, Entwicklung, Globalisierung, Gewalt und Sicherheit.

Verkauf der GIGA-Datenbank in einem Hacker-Forum

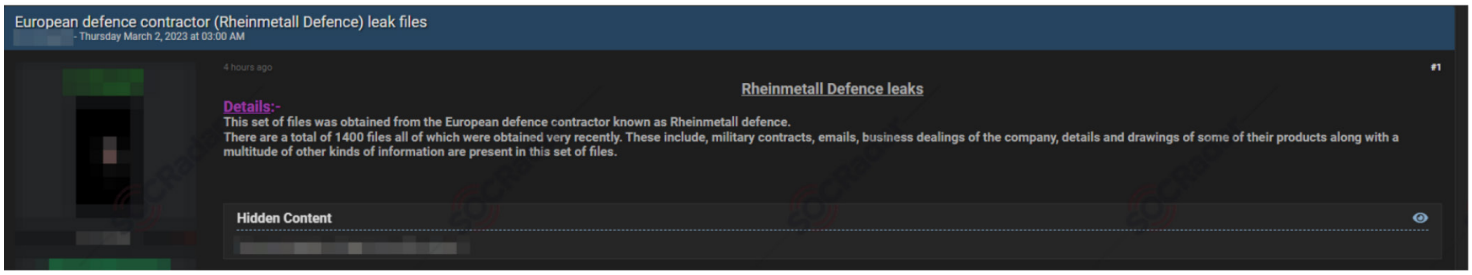
Am 24. Februar 2023 wurde ein neues Datenleck entdeckt, das deutsche WhatsApp-Nutzer betrifft. Die durchgesickerten Daten enthalten eine Liste von 50.000 verifizierten WhatsApp-Nummern.



Deutsche WhatsApp-Bentzerleck im Dark-Web-Forum

Jüngste Aktivitäten im Dark Web, die auf Einrichtungen in Deutschland abzielen

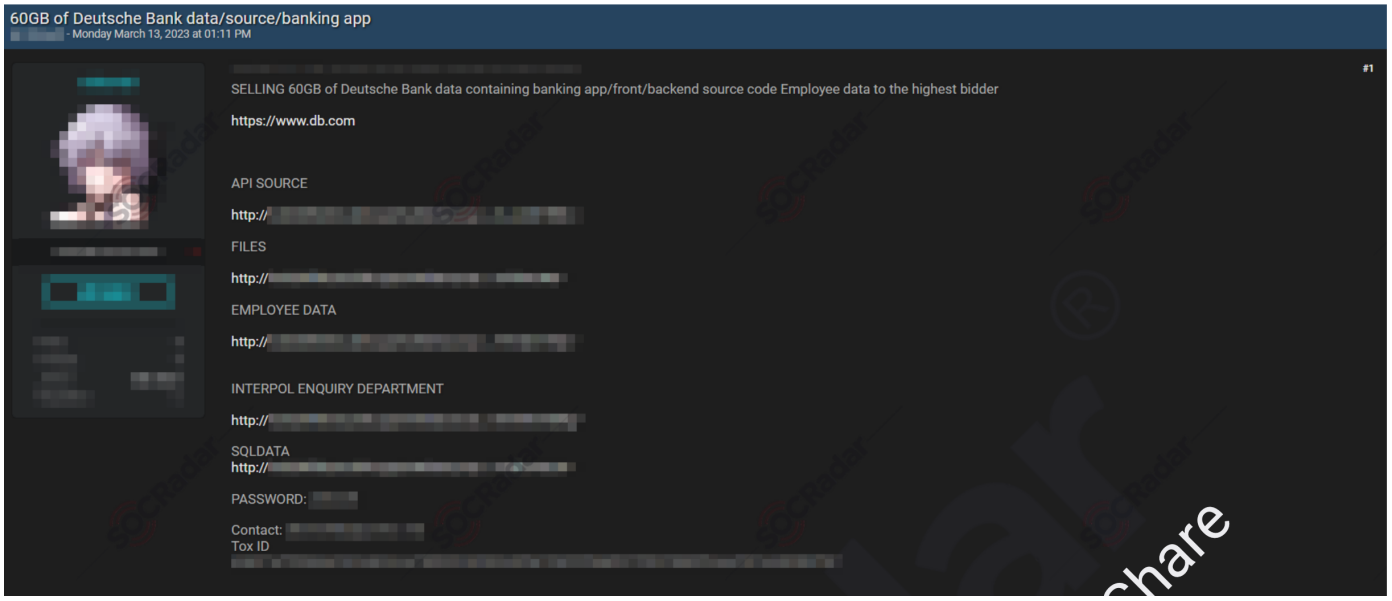
Am 2. März 2023 wurde ein neues Leck mit sensiblen Dokumenten der Rheinmetall AG, einem deutschen Automobil- und Rüstungshersteller mit Sitz in Düsseldorf, entdeckt. Das Leck enthält Berichten zufolge 1.400 Dateien, darunter militärische Verträge, E-Mails, Geschäftsvorgänge und detaillierte Produktinformationen.



Sensible Informationen der Rheinmetall AG im Dark-Web-Forum veröffentlicht

Darüber hinaus wurde die Rheinmetall AG am 20. Mai 2023 als neues Ransomware-Opfer bekannt gegeben, laut der ebenfalls von SOCRadar beobachtete Website der Gruppe Black Basta ransomware. Da dieser Ransomware-Angriff nach dem Datenleck erfolgte, ist naheliegend, dass, die meisten Unternehmen mehr als einmal gehackt wurden.

Am 13. März 2023 wurde ein weiteres mutmaßliches Datenleck bei der Deutschen Bank entdeckt. Die Daten, die dem Höchstbietenden zum Kauf angeboten wurden, enthalten 60 GB an Informationen, darunter Quellcode von Bankanwendungen, Mitarbeiterdaten, Details der Interpol-Auskunftsabteilung, SQL-Daten und Passwörter.



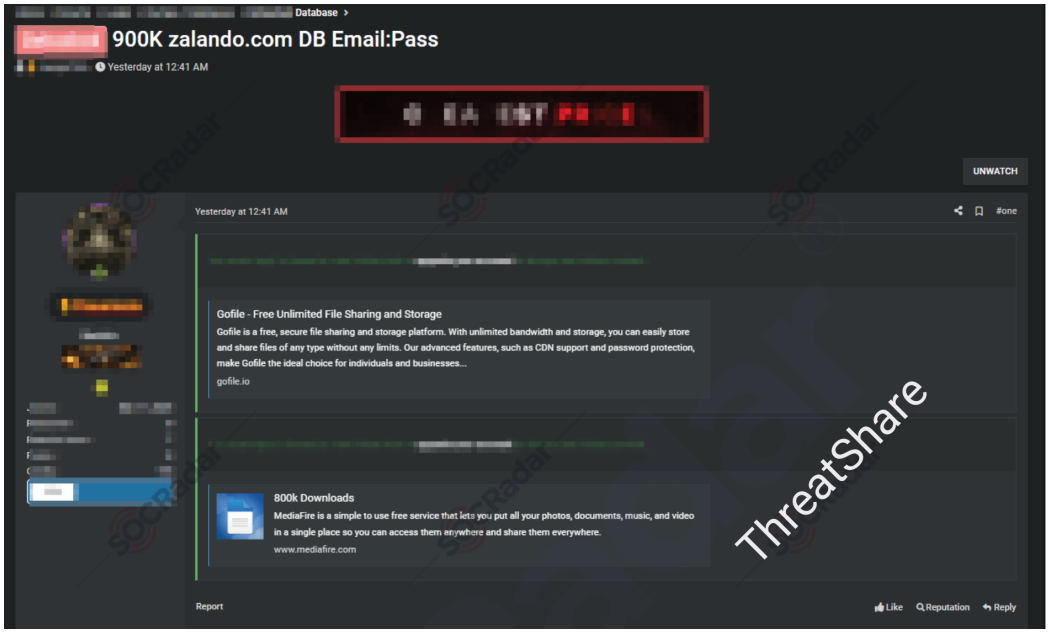
Datenleck von sensiblen Informationen der Deutschen Bank im Dark Web Forum veröffentlicht

Jüngste Aktivitäten im Dark Web, die auf Einrichtungen in Deutschland abzielen

Am 18. März 2023 wurde in einem von SOCRadar überwachten Hackerforum ein neues Verkaufsangebot für Kundendaten der Deutschen Telekom entdeckt. Das Datenleck ist vom November 2022. Die Daten enthalten Details zu 27,3 Millionen deutschen Kunden der Deutschen Telekom, darunter Name, Nachname, Wohnadresse und Telefonnummer. Die Deutsche Telekom AG ist ein deutsches Telekommunikationsunternehmen mit Hauptsitz in Bonn und gemessen am Umsatz der größte Telekommunikationsanbieter in Europa.

Verkauf der Deutschen Telekom-Datenbank im Dark Web Forum

Am 22. März 2023 wurde in einem von SOCRadar überwachten Hackerforum ein neues Datenbankleck bei Zalando entdeckt. Die Zalando SE ist ein börsennotierter deutscher Online-Händler für Schuhe, Mode und Schönheit, der in ganz Europa aktiv ist und mehr als 51 Millionen aktive Nutzer in 25 europäischen Märkten hat.

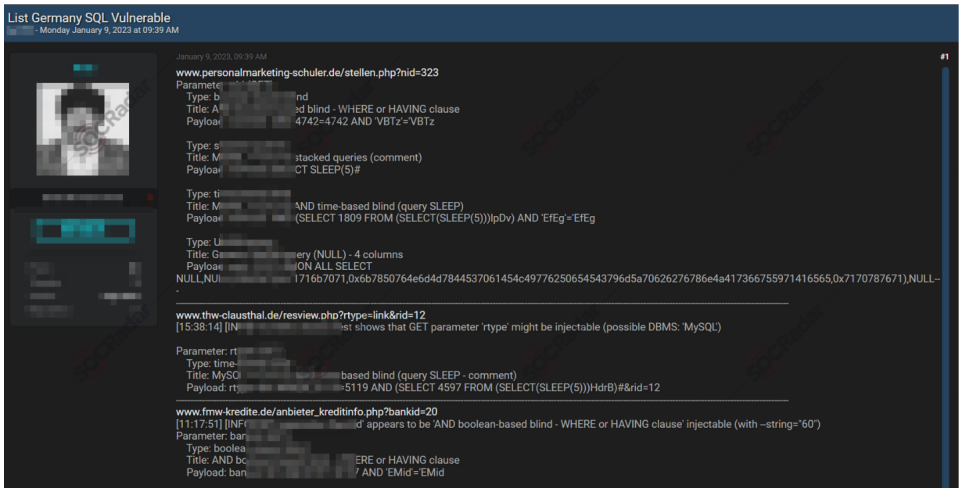


Verkauf der Zalando-Datenbank im Dark Web Forum

Jüngste Aktivitäten im Dark Web, die auf Einrichtungen in Deutschland abzielen

Software-Schwachstellen (Zero-Days, SQL-Injection-Schwachstellen etc.)

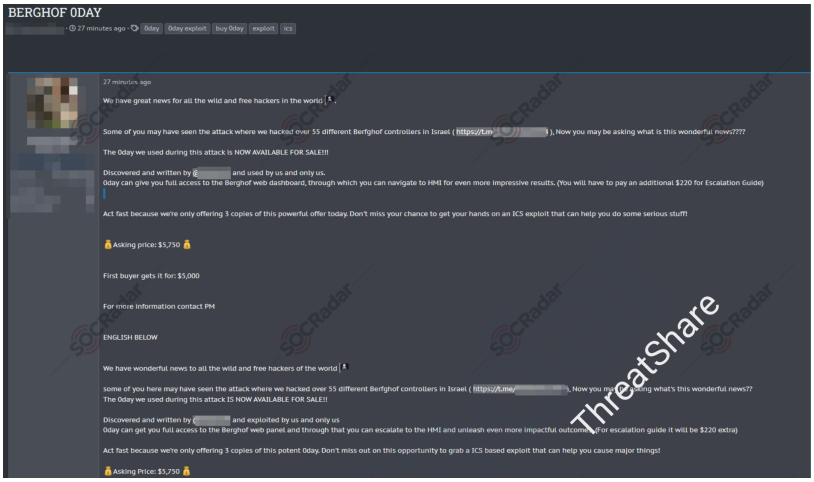
Am 9. Januar 2023 wurde in einem von SOCRadar überwachten Hackerforum eine neue SQL-Injection-Schwachstelle für viele deutsche Websites entdeckt. Ein SQL-Injection-Angriff besteht aus der Eingabe einer SQL-Abfrage über die Eingabedaten vom Client in die Anwendung. Ein erfolgreicher SQL-Injection-Angriff kann sensible Daten aus der Datenbank auslesen und Datenbankdaten verändern.



Im Dark-Web-Forum gefundene deutsche Webseiten mit SQL-Injection-Schwachstellen

Am 27. Mai 2023 wurde in einem von SOCRadar überwachten Hackerforum der Verkauf eines neuen 0-Day-Exploits für Berghof Automation entdeckt. Die Berghof Automation GmbH ist ein Hersteller von Fabrikautomationsanlagen. Das Unternehmen bietet automatisierte Produktionssysteme für die Chemie-, Logistik-, Schwerindustrie und den Maschinenbau an und beliefert Kunden weltweit.

Der Bedrohungsakteur berief sich auf einen Angriff in Israel, bei dem er mehr als 55 verschiedene Berghof-Steuerungen hackte und die 0-Day-Schwachstelle für 5.750 US-Dollar zum Verkauf anbot. Für zusätzliche 220 $ konnten Käufer vollen Zugang zum Berghof-Web-Control-Panel 220 erhalten, um Zugriff auf den Eskalationsleitfaden zu erhalten.



Berghof Automation GmbH Zero-Day-Schwachstelle im Dark-Web-Forum

Jüngste Aktivitäten im Dark Web, die auf Einrichtungen in Deutschland abzielen

Zugang: Verwaltung/RDP/VPN/Netzwerk/Shell

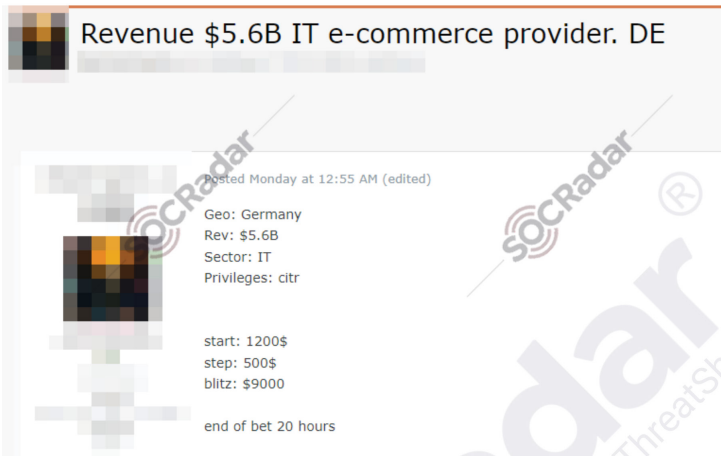
Am 20. Februar 2023 wurde in einem von SOCRadar überwachten Hackerforum ein unautorisierter VPN-Zugang zum Verkauf angeboten, der einem deutschen Produktionsunternehmen gehörte. Die Benutzerrechte für den VPN-Zugang des Unternehmens, das in der Industrieelektronik-Branche mit 20.000 Mitarbeitern und einem Umsatz von 5,5 Milliarden US-Dollar tätig ist, wurde von den Cyberangreifern zu einem Preis ab 1.500 US-Dollar versteigern.

Unautorisierter VPN-Zugang bei deutschem Fertigungsunternehmen im Dark-Web-Forum entdeckt

Am 30. April 2023 wurde in einem von SOCRadar überwachten Hackerforum ein Verkauf von unautorisierten Admin-Zugängen entdeckt, die einem in Deutschland tätigen Elektrounternehmen gehören. Es wird behauptet, dass die VPN- und lokalen Admin-Berechtigungen des Unternehmens, das in Deutschland kommerzielle Dienstleistungen für Elektroinstallations- und Stahlunternehmen sowie Betonbauhersteller anbietet, ab 499 Dollar versteigert werden.

Unautorisierter Admin-Zugang bei deutschem Elektrounternehmen im Dark-Web-Forum gefunden

Am 26. Juni 2023 wurde in einem von SOCRadar überwachten Hackerforum der Verkauf eines nicht autorisierten Netzwerkzugangs entdeckt, der einem in Deutschland tätigen E-Commerce-Unternehmen gehört. Es wird davon ausgegangen, dass es sich bei dem Unternehmen, dessen Active Directory Domain Admin Rechte ebenfalls zu einem Preis ab 1.200 Dollar versteigert werden, um einen E-Commerce-Riesen handelt, der in der IT-Branche tätig ist und einen Umsatz von 5,6 Milliarden Dollar erzielt.



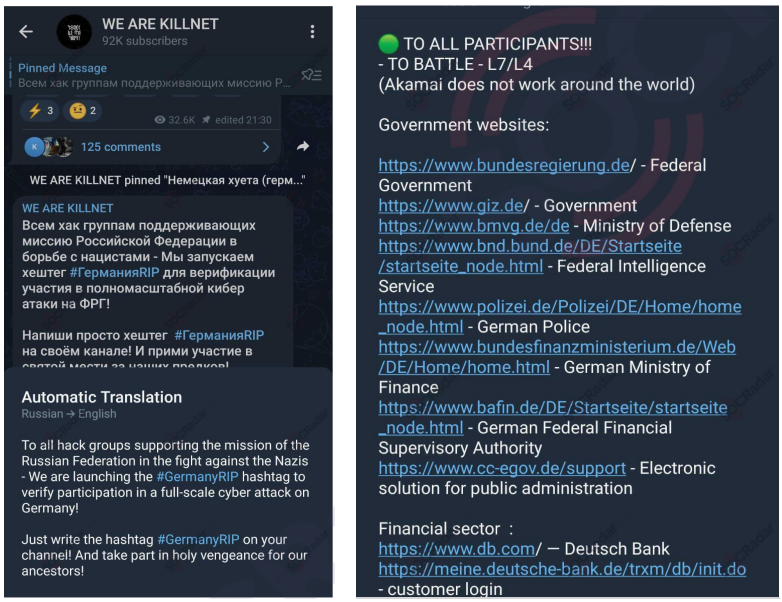
Unbefugter Netzwerkzugang bei deutschem E-Commerce-Unternehmen im Dark-Web-Forum entdeckt

Jüngste Aktivitäten im Dark Web, die auf Einrichtungen in Deutschland abzielen

Sonstige (Stealer Logs, Tools & Dienste, Botnetze, Exploits, DDoS-Angriffe)

Am 26. Januar 2023 griff die pro-russische Hackergruppe KillNet mit einer koordinierten DDoS-Kampagne (Distributed Denial of Service) Regierungswebsites, Banken und Flughäfen an.

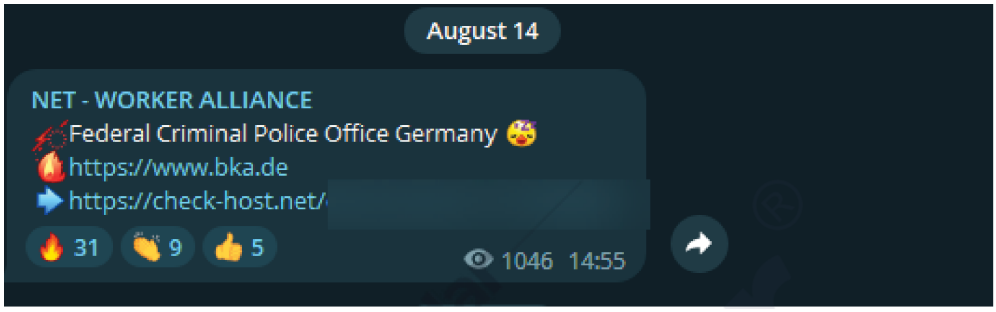
Sie kündigten die Einführung des Hashtags #GermanyRIP



Killnet-Ankündigung richtet sich an deutsch öffentliche und private Einrichtungen

Am 14. August 2023 entdeckte das Dark-Web-Team von SOCRadar eine alarmierende Ankündigung auf dem Telegram-Kanal der Angreifergruppe NET-WORKER ALLIANCE. In der Ankündigung wurde behauptet, dass sie erfolgreich einen DDoS-Angriff auf die Website des deutschen Bundeskriminalamtes durchgeführt hätten. NET-WORKER ALLIANCE ist kein Neuling in der Veröffentlichung solcher Ankündigungen; die Gruppe mit ihrer pro-russischen Haltung hat sich bereits früher für Angriffe auf wichtige europäische Institutionen wie Europol und CYBERPOL verantwortlich gemacht.

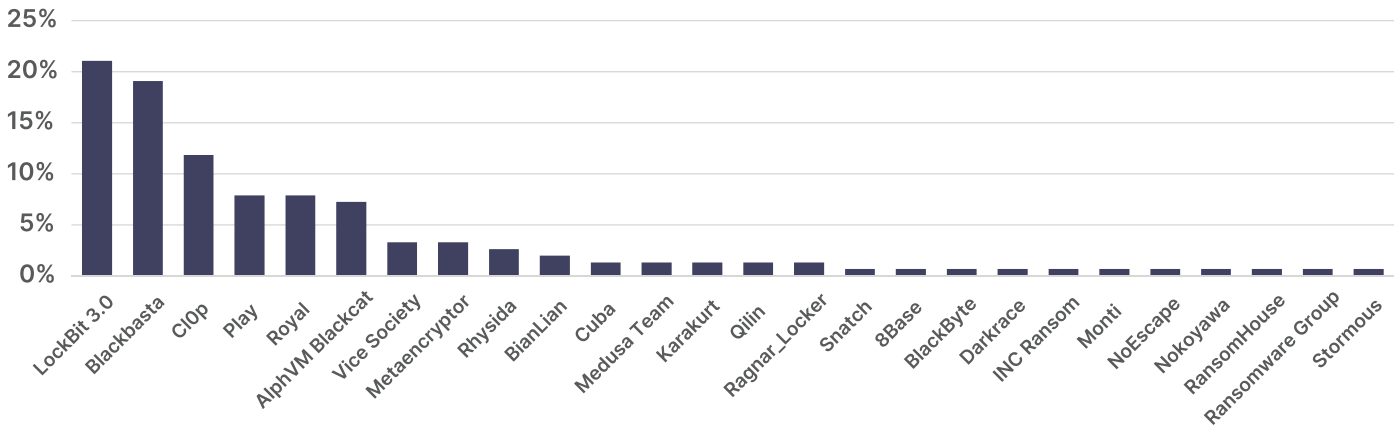
Das Kollektiv bildete am 29. Juli eine Allianz, die als Zusammenschluss mehrerer Bedrohungsakteure entstand: BLOODNET, Phoenix, BlueNet, CyberCat, unkn0wn und Contagio. Ihre Beweggründe scheinen klar: Sie wollen ihre Kräfte bündeln, weitere pro-russische Cyber-Akteure in die Gemeinschaft einbinden und ihre Offensivfähigkeiten ausbauen - insbesondere in den Bereichen DDoS, Defacement und Penetration.



NET-WORKER ALLIANCE Beitrag über DDoS-Angriff auf das Bundeskriminalamt

Die wichtigsten Ransomware-Gruppen, die auf deutsche Unternehmen abzielen

Während eines Zeitraums von 12 Monaten registrierte die SOCRadar XTI-Plattform 152 Ransomware-Vorfälle, die auf Unternehmen in Deutschland abzielten. Diese Plattform wird kontinuierlich mit Daten aus Untergrundforen und Telegram-Kanälen gefüttert, die vom SOCRadar Dark Web Team überwacht und verfolgt werden. Im gleichen Zeitraum wurden 26 verschiedene Ransomware-Gruppen identifiziert, die diese Cyberangriffe durchgeführt haben.



Nachfolgend finden Sie die Top-5-Liste der Ransomware-Gruppen, die auf Unternehmen in Deutschland abzielen, basierend auf Daten aus den letzten 12 Monaten:

- LockBit 3.0
- Blackbasta
- Cl0p
- Play & Royal Ransomware
- AlphVM Blackcat

Die wichtigsten Ransomware-Gruppen, die auf deutsche Unternehmen abzielen

Die Verteilung der Branchen, die im letzten Jahr Ziel von Ransomware-Angriffen waren, ist in der folgenden Grafik dargestellt. Es ist ersichtlich, dass mehr als 20 Branchen und Teilbranchen erfolgreichen Ransomware-Angriffen zum Opfer gefallen sind. Praktisch keine Branche bleibt von Ransomware-Bedrohungen unberührt, was zu der Schlussfolgerung führt, dass Anwendungen, die über das Internet zugänglich sind, unabhängig von der Branche potenziell im Visier von Cyber-Angreifern sind.

Die 5 am häufigsten angegriffenen Branchen sowie die Anzahl der Angriffe für jede Branche sind ebenfalls unten aufgeführt.

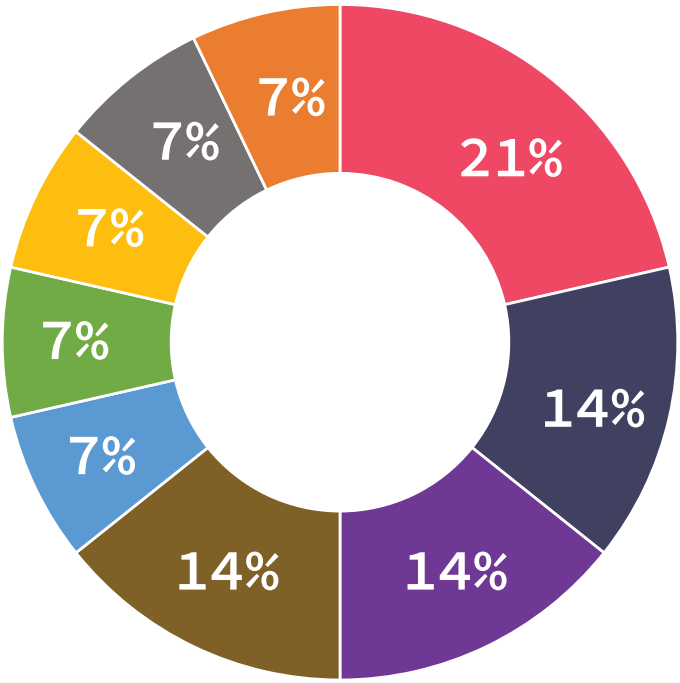
1. **Fertigungsunternehmen (46)**
2. **Freiberufliche-, wissenschaftliche- und technische Dienstleistungs-Unternehmen (18)**
3. **Sonstige Dienstleistungen (außer öffentliche Verwaltung) (14)**
4. **IT-Unternehmen (13)**
5. **5- Einzelhandel (13)**

Am häufigsten angegriffenen Branchen

Die wichtigsten Ransomware-Gruppen, die auf deutsche Unternehmen abzielen

Das nachstehende Schaubild zeigt eine Aufschlüsselung und Verteilung der Branchen in der Kategorie Sonstige Dienstleistungen (“Others”), die an dritter Stelle der am stärksten angegriffenen Branchen steht.

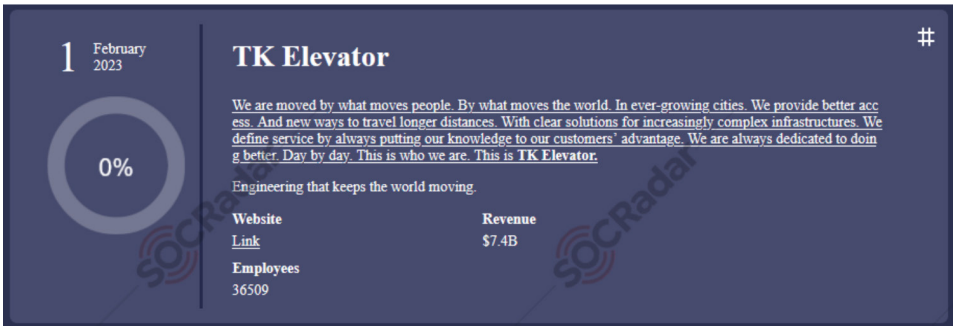
Aufschlüsselung und Verteilung der Branchen in der Kategorie Sonstige Dienstleistungen (“Others”)



- Accommodation and Food Services
- Religious, Grantmaking, Civic, Professional, and Similar Organizations
- Other Services (except Public Administration), Repair and Maintenance
- Clothing Stores
- Real Estate and Rental and Leasing
- Public Administration
- Mining, Quarrying, and Oil and Gas Extraction
- Legal Services
- Health Care and Social Assistance

Bekannte Ransomware-Angriffe im Jahr 2023

Am 1. Februar 2023 wurde auf der Website der Ransomware-Gruppe Royal ein neues Opfer angekündigt: TK Elevator. TK Elevator GmbH, auch bekannt als ThyssenKrupp Elevator, ist ein Unternehmen, das Aufzüge, Fahrtreppen, Fahrsteige und Lösungen für Barrierefreiheit herstellt. Das Unternehmen ist derzeit der viertgrößte Aufzughersteller der Welt und beliefert Kunden in über 100 Ländern.



Royal Ransomware Opfer: TK Elevator

Am 5. März 2023 überwachte SOCRadar die Website der Ransomware-Gruppe Vice Society und entdeckte neue Datenlecks, die zur HAW Hamburg gehörten. Die HAW Hamburg ist derzeit die zweitgrößte Hochschule in Hamburg und eine der größten Hochschulen für angewandte Wissenschaften in Deutschland. Die Hochschule bietet praxisnahe Studiengänge in Fächern wie IT, Biowissenschaften, Design, Medien, Wirtschaft und Sozialwissenschaften an, wobei die Professoren aus verschiedenen relevanten Branchen kommen.

Vice Society Ransomware Opfer: HAW HAMBURG

Am 23. Mai 2023 wurde auf der ebenfalls von SOCRadar überwachten Webseite der Play Ransomware-Gruppe ein neues Ransomware-Opfer angekündigt: Black Cat Networks. Das Unternehmen bietet seit 2007 verwalteten Support für Computernetzwerkinfrastrukturen vor Ort an. Der Bedrohungsakteur gab bekannt, dass er über vertrauliche Daten verfügt, darunter Kunden- und Mitarbeiterdokumente, Finanzunterlagen und Steuerinformationen, und drohte damit, diese innerhalb von drei Tagen offenzulegen, wenn das Lösegeld nicht gezahlt wird.

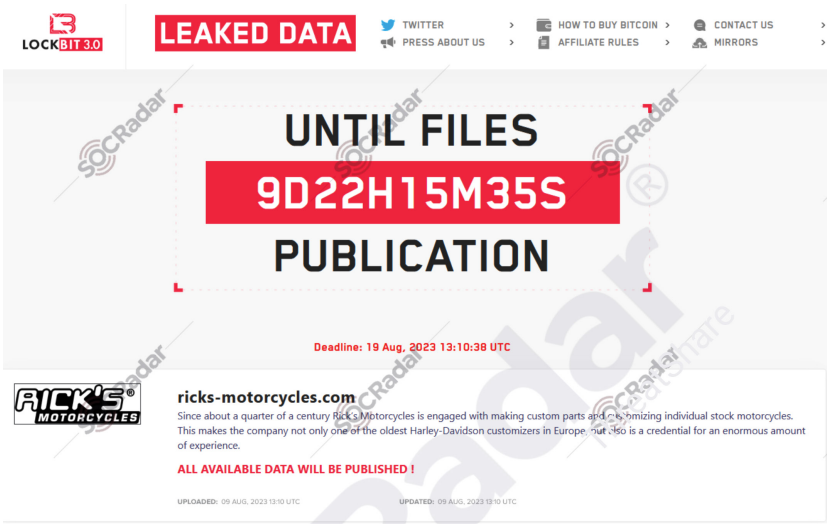
Play Ransomware-Opfer: Black Cat Networks

Bekannte Ransomware-Angriffe im Jahr 2023

Am 26. Juni 2023 kündigte die von SOCRadar überwachte Webseite der Ransomware-Gruppe Cl0p ein neues Ransomware-Opfer an: Siemens Energy. Die Siemens Energy AG ist ein Energieunternehmen, das durch die Ausgliederung der ehemaligen Gas- und Stromsparte der Siemens AG entstanden ist. Die Produktpalette des Konzerns umfasst hauptsächlich Stromübertragung und -verteilung, Generatoren, Kraftwerkstechnik, Niederspannungsschaltanlagen, Turbinen (einschließlich Wind-, Dampf- und Gasturbinen), Kompressoren und Elektrolyseure.

Cl0p Ransomware Opfer: Siemens Energie

Am 9. August 2023 gab die ebenfalls von SOCRadar überwachte Website der Ransomware-Gruppe LockBit 3.0 ein neues Opfer bekannt: Rick's Motorcycles. Seit etwa einem Vierteljahrhundert beschäftigt sich Rick's Motorcycles mit der Herstellung von Sonderteilen und der individuellen Anpassung von Serienmotorrädern. Diese Erfahrung macht das Unternehmen nicht nur zu einem der ältesten Harley-Davidson-Customizer in Europa, sondern spricht auch für seine umfassende Expertise in diesem Bereich.



Lockbit 3.0 Ransomware-Opfer: Rick's Motorcycles

Die 5 wichtigsten Bedrohungsakteure, die es auf deutsche Organisationen abgesehen haben

Laut den Forschungsergebnissen von SOCRadar wird Deutschland im Jahr 2023 von hochentwickelten Cyberangriffen betroffen sein, insbesondere von Advanced Persistent Threat (APT)-Gruppen. Im Folgenden finden Sie einige wichtige Informationen über fünf der prominentesten Bedrohungsakteure der hochgefährlichen Kategorie:

Die in China ansässige Bedrohungsgruppe Ice Frog führt seit mindestens 2011 aktive Cyber-Spionagekampagnen durch. Sie zielt hauptsächlich auf Regierungsbehörden, militärische Auftragnehmer, Schifffahrts- und Schiffsbauunternehmen, Telekommunikations- und Satellitenbetreiber, Industrie- und Hightech-Unternehmen sowie Medien in Südkorea und Japan ab. Darüber hinaus zielt die Gruppe auf Organisationen in westlichen Ländern wie den Vereinigten Staaten, Deutschland und anderen Teilen Europas ab.

Die in Russland ansässige Bedrohungsgruppe Turla, auch bekannt als Snake, ist eine hochentwickelte APT-Gruppe, die sich auf Spionage und das Sammeln von Informationen konzentriert. Turla ist seit den späten 1990er Jahren aktiv und gilt als eines der frühesten Beispiele für Cyberspionage. Die Gruppe hat es vor allem auf Regierungsstellen, militärische Organisationen und Botschaften abgesehen.

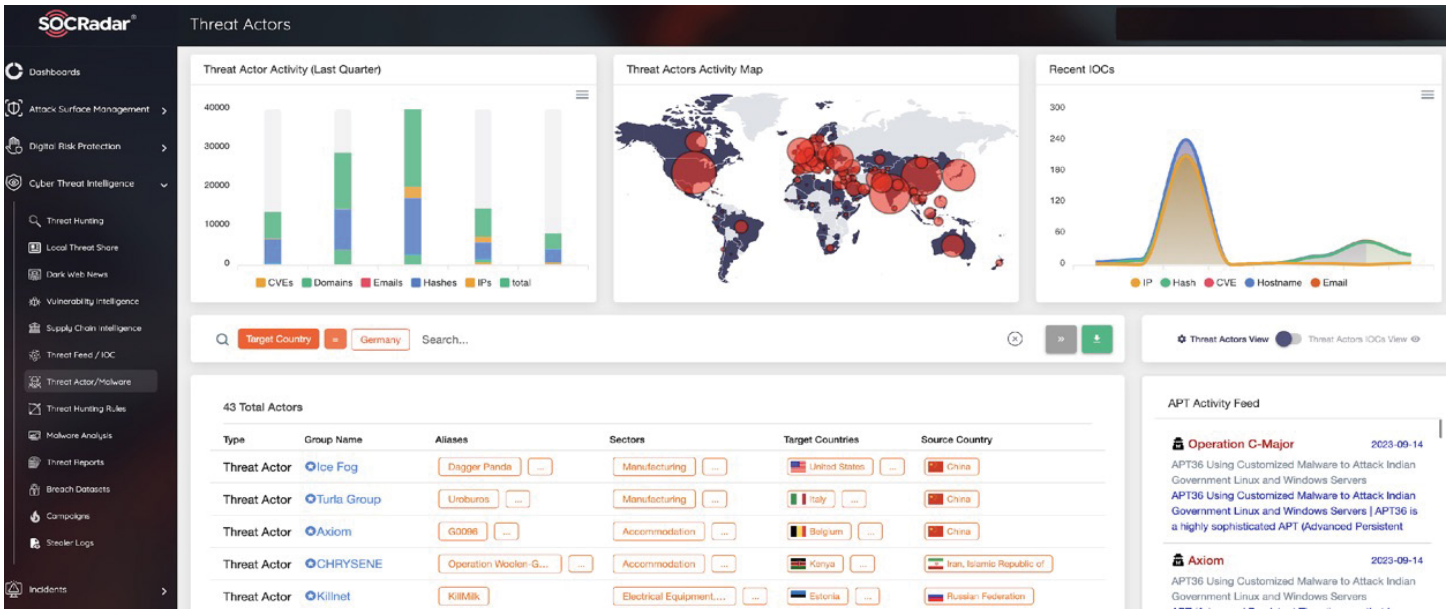
Ein neuer, finanziell motivierter Bedrohungsakteur, TA866, ist seit Oktober 2022 aktiv. Er zielt auf Organisationen in den USA und Deutschland ab. Die Angriffskette beginnt in der Regel mit einer bösartigen E-Mail, die einen Anhang oder eine URL enthält und zur Installation von Malware wie WasabiSeed und Screenshotter führt. TA866 ist ein organisierter Akteur, der in der Lage ist, seine Angriffe zu skalieren und sich dabei auf seine eigenen Tools und die Möglichkeit, Tools und Dienstleistungen von anderen Anbietern zu erwerben, zu stützen.

Die 5 wichtigsten Bedrohungsakteure, die es auf deutsche Organisationen abgesehen haben

Charming Kitten (auch bekannt als APT35) ist eine der iranischen Regierung nahestehende Gruppe für Cyber-Kriegsführung. Sie wird von verschiedenen Unternehmen und Regierungsvertretern als Advanced Persistent Threat (APT) eingestuft und zielt in erster Linie auf militärisches-, diplomatisches- und Regierungspersonal in den USA, Westeuropa und dem Nahen Osten ab. Weitere Ziele der Gruppe sind die Bereiche Medien, Energie, Verteidigung, Technik, Unternehmensdienstleistungen und Telekommunikation.

KillNet ist eine pro-russische Hackergruppe, die während der russischen Invasion in der Ukraine im Jahr 2022 bekannt wurde. Sie ist nach wie vor aktiv und bekannt für ihre DDoS-Angriffe (Distributed Denial of Service) gegen Regierungsbehörden und Privatunternehmen, insbesondere in NATO-Ländern.

In Anbetracht der Tatsache, dass Bedrohungsakteure ihre Opfer oft anhand verschiedener Kriterien auswählen und sich auf bestimmte Branchen konzentrieren, sind kontextbezogene Informationen, die mit Dark Web Intelligence angereichert sind, von entscheidender Bedeutung. Informationen über die sich ändernden Taktiken, Techniken und Verfahren (TTPs = tactics, techniques, and procedures) sowie Malware-Kampagnen aus dem SOCRadar-Modul Threat Actors können für proaktive Maßnahmen von unschätzbarem Wert sein.

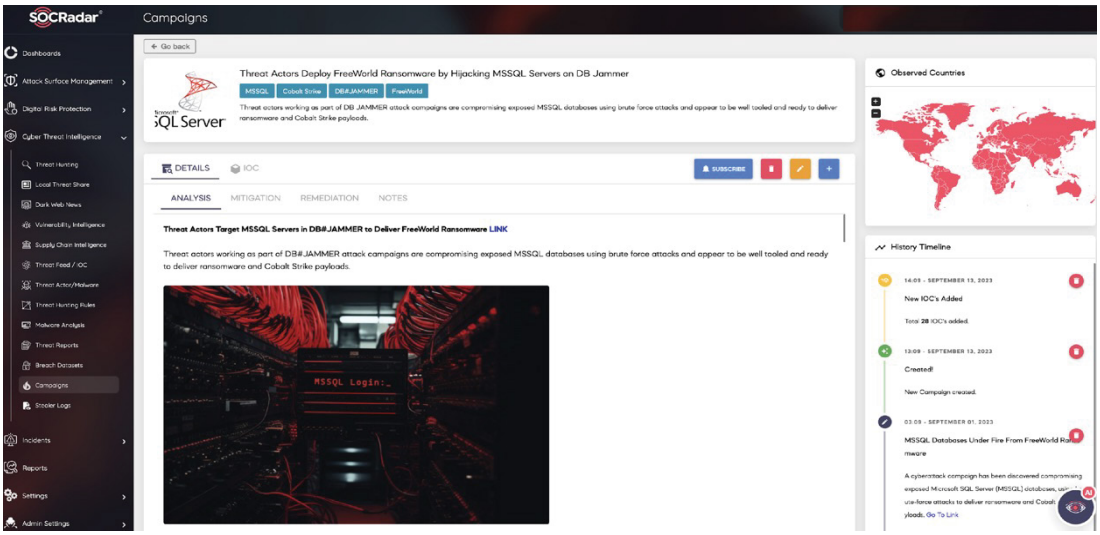


SOCRadar Bedrohungsakteure/ Malware-Modul

Die 5 wichtigsten Bedrohungsakteure, die es auf deutsche Organisationen abgesehen haben

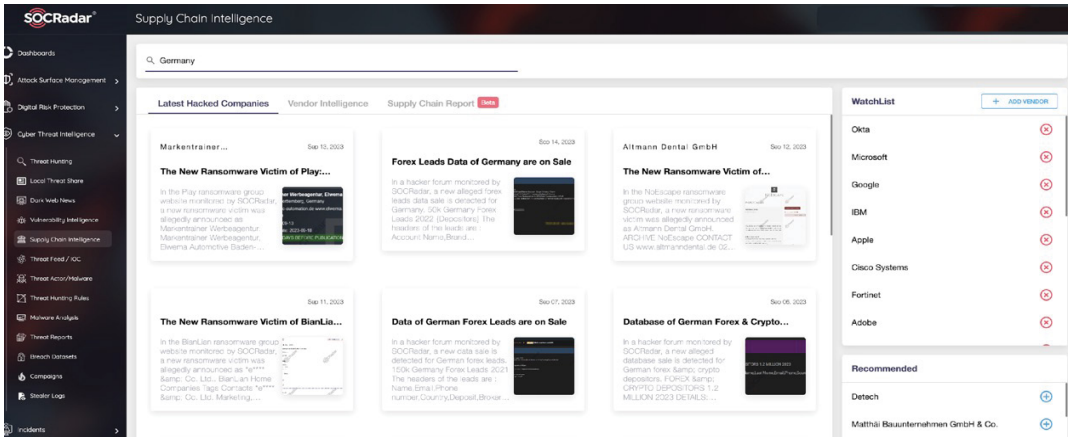
Darüber hinaus bietet die SOCRadar-Kampagnenseite, die Dark Web und Open-Source Intelligence (OSINT) kombiniert, Informationen über die jüngsten Angriffsaktivitäten, die zeitlich genau abgestimmt wurden, erfolgreich waren und sich weiter ausbreiten.

Nachrichtendienstliche Informationen über diese Kampagnen können für Ihr Unternehmen von entscheidender Bedeutung sein. Kampagnen können als eine Reihe von nicht autorisierten Angriffsversuchen definiert werden, die im Laufe der Zeit gemeinsame Ziele verfolgen. Diese Aktivitäten können, müssen aber nicht direkt mit einem bestimmten Bedrohungsakteur verbunden sein. Daher können Sie diese Bedrohungselemente, die sich über ein bestimmtes Gebiet ausbreiten, über die SOCRadar-Kampagnenseite verfolgen.



SOCRadar-Kampagnenseite

Darüber hinaus sind Angriffe über die Lieferkette eine neue Bedrohung, die zur Verbreitung von Malware genutzt wird, indem vertrauenswürdige, legitime Anwendungen infiziert werden. Diese Angriffe nutzen oft Unternehmen mit schwachen Sicherheitsvorkehrungen aus. Daher kann das SOCRadar-Modul "Supply Chain Intelligence" Sie auf Unternehmen aufmerksam machen, die bereits Cyberangriffen ausgesetzt sind, verwertbare Informationen aus vergangenen Vorfällen und Datenschutzverletzungen von Anbietern extrahieren und Ihnen einen mit Erkenntnissen über Bedrohungen angereicherten Bericht zur Verfügung stellen.



SOCRadar Modul für Lieferketten-Intelligenz

Fazit und Empfehlungen

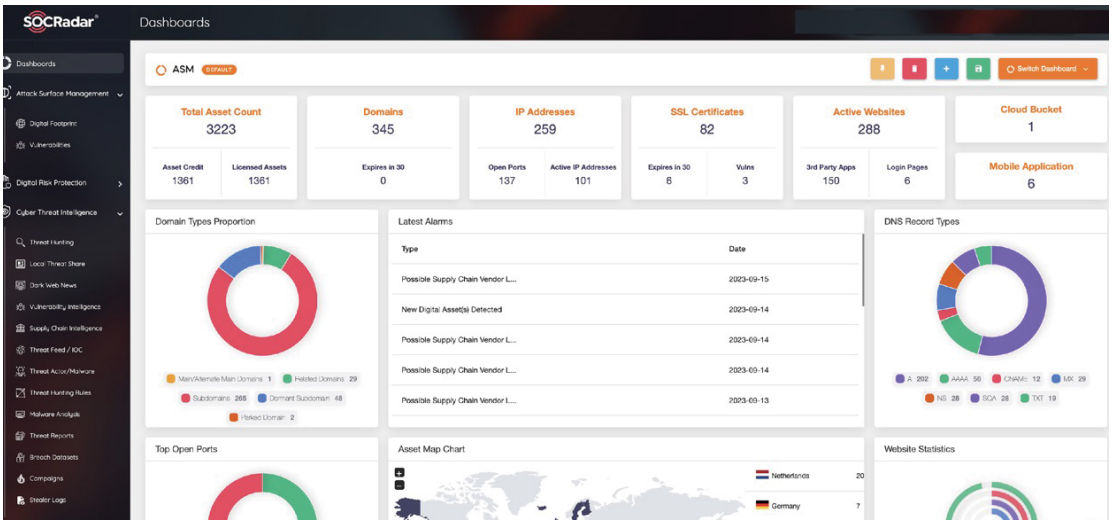
Obwohl Deutschland seinen Platz unter den wirtschaftlich entwickelten Ländern behauptet, ist es zu einem der Hauptziele von Cyber-Bedrohungsakteuren geworden und ist von Cyber-Risiken erheblich betroffen. Das Aufkommen von Industrie 4.0 und die Inbetriebnahme von cyber-physischen Systemen haben die Sicherheitsbedenken in Branchen, die für die wirtschaftliche Entwicklung entscheidend sind, wie z. B. die Fertigungsunternehmen, besonders verstärkt.

Laut den Forschungsergebnissen von SOCRadar zielen die Hälfte der Attacken auf Fertigungsunternehmen den Fokus auf die Automobilbranche, in der Deutschland weltweit führend ist. Darüber hinaus hat die Zunahme von Ransomware-Angriffen schwere Auswirkungen auf deutsche Unternehmen. Unternehmen mit einem Umsatz in Milliardenhöhe sind Opfer von Hackerangriffen geworden. Daher ist es von entscheidender Bedeutung, die Cybersicherheitsmaßnahmen zu verstärken, insbesondere in neuen Bereichen wie Cyber Threat Intelligence (CTI), indem ein hochmoderner Sicherheitsansatz verfolgt und eine proaktive Sicherheitsagenda für Unternehmen festgelegt wird.

Im Vergleich zu den Daten aus dem Jahr 2022 wurden ältere Bedrohungsakteure durch neue ersetzt (z. B. der Übergang von LockBit 2.0 zu LockBit 3.0), und die Zahl der Bedrohungsakteure, die es auf Deutschland abgesehen haben, ist gestiegen, insbesondere durch Ransomware-Angriffe. Während das Volumen der Angriffe auf verschiedene Branchen quantitativ relativ stabil geblieben ist, ist die Zahl der betroffenen Branchen um 33 % gestiegen. Darüber hinaus ist ein deutlicher Anstieg der finanziellen und rufschädigenden Schäden für größere Unternehmen zu verzeichnen.

Auf der Grundlage dieser Forschungsergebnisse sind die folgenden Empfehlungen für deutsche Unternehmen von entscheidender Bedeutung:

- Digitale Angriffsflächen sollten genau definiert und durch Attack Surface Management (ASM) Services verwaltet werden. Diese Dienste decken Ihre digitalen Assets auf, bewerten und helfen, Ihr Cybersecurity-Risiko zu mindern. ASM-Dienste sind entscheidend für das Verständnis und die Sichtbarmachung Ihrer wachsenden Angriffsfläche, indem sie Sie auf relevante Schwachstellen hinweisen.

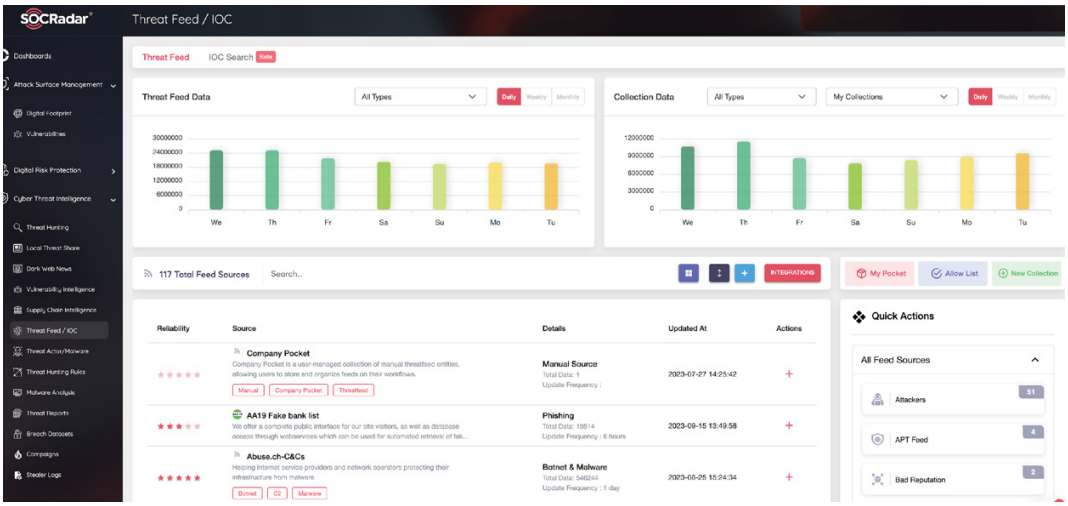


SOCRadar Modul zur Verwaltung der Angriffsfläche

Fazit und Empfehlungen

- Wir stellen fest, dass Unternehmen Cyber-Vorfälle wie Datenschutzverletzungen loft erst lange nach dem Eindringen in ihre Daten entdecken. Um diesen reaktiven Ansatz in eine proaktive Strategie umzuwandeln, sollten Unternehmen eine Security Operations Center (SOC) Infrastruktur nutzen. Diese Infrastruktur sollte durch Cyber Threat Intelligence (CTI)-Feeds gespeist werden, die den Sicherheitsanalysten verwertbare Erkenntnisse aus dem Dark Web liefern und letztlich die Fähigkeiten zur Erkennung und Reaktion auf Cyber-Bedrohungen zusammenführen.

  Das SOCRadar-Modul "Threat Feed and Indicator of Compromise (IoC) Management" unterstützt Cybersecurity-Teams durch die Bereitstellung angereicherter Daten über benutzerfreundliche Dashboards. Cybersicherheitsexperten können diese Feeds anpassen, um über die neuesten Bedrohungen auf dem Laufenden zu bleiben, nach IOCs (Indicators of Compromise, IoCs) zu suchen und sie über das TAXII-Protokoll in Unternehmenssysteme zu integrieren.

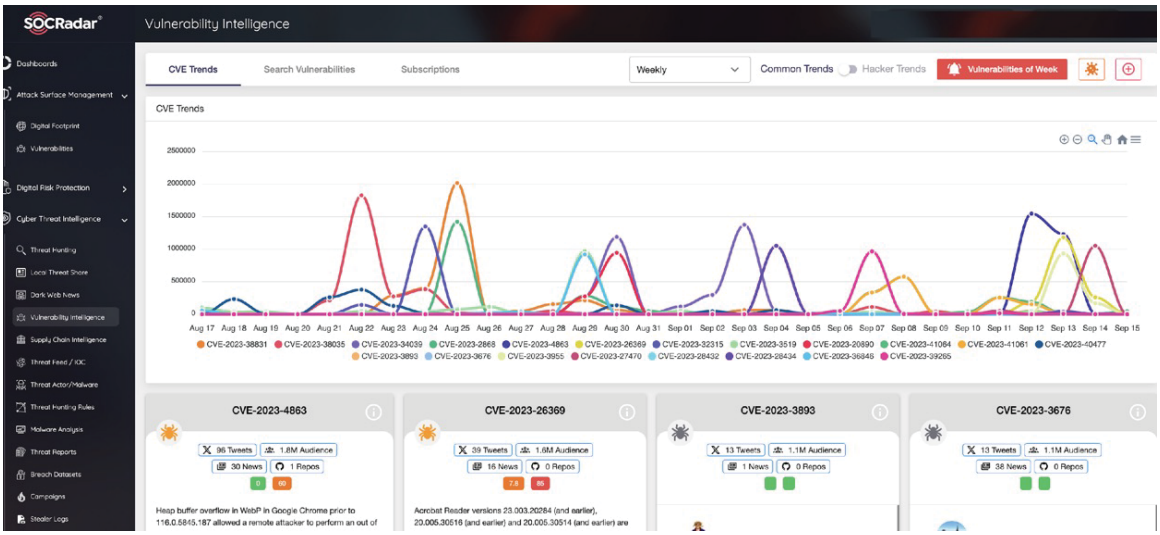


SOCRadar Bedrohungs-Feed/ IOC-Verwaltungsmodul

Fazit und Empfehlungen

- Da es Anzeichen dafür gibt, dass Bedrohungsakteure, insbesondere Ransomware-Gruppen, immer mehr Schwachstellen ausnutzen, ist es von entscheidender Bedeutung, der Patch-Management Priorität einzuräumen und Patches zeitnah zu installieren. Da die Häufigkeit bekannter ausgenutzter Schwachstellen zunimmt, sollten Datenbanken wie der KEV-Katalog (Known Exploited Vulnerabilities) der CISA kontinuierlich überwacht und Maßnahmen so schnell wie möglich ergriffen werden..

  Mit dem Vulnerability Intelligence-Modul von SOCRadar erhalten Sie Einblicke in die Schwachstellen, die von Bedrohungsakteuren ausgenutzt werden, und können Trends erkennen. Kontextbezogene und umsetzbare Informationen über potenziell gefährdete Technologien können verwendet werden, um Risikobewertungen und Informationsvalidierungsprozesse zu beschleunigen.



SOCRadar Modul für Schwachstellenanalyse

Wer ist SOCRadar®?

Your Eyes Beyond

SOCRadar bietet Extended Cyber Threat Intelligence (XTI), die Folgendes kombiniert: ***"Cyber Threat Intelligence, Digital Risk Protection und External Attack Surface Management Services."*** SOCRadar bietet den umsetzbaren und zeitnahen Informationskontext, den Sie benötigen, um die Risiken im Transformationszeitalter zu bewältigen.

SOCRadar bietet Schutz vor Bedrohungen für mehr als 12.000 Unternehmen aus 157 Ländern und ist zu einer Erweiterung von SOC-Teams aus allen Branchen geworden.

12.000
Kostenlose Benutzer

LERNEN SIE DIE NEUE MOBILE APP

Greifen Sie auf Bedrohungsinformationen zu, ergreifen Sie unterwegs Maßnahmen und werden Sie sofort über neue Bedrohungen benachrichtigt. Sehen Sie sich Warnungen, aktuelle Dark-Web-Nachrichten und neue Ransomware-Angriffe an

Download on the App Store

GET IT ON Google Play

Gartner Peer Insights™ 4.9/5