VARGROUP

Pressemitteilung [7.831 Zeichen inkl. Leerzeichen]

Fertigungsindustrie ist Ziel Nr. 1

Bericht der Var Group zu Cyberangriffen auf deutsche Unternehmen und Organisationen veröffentlicht

München, 24.06.2025 – Das Cyber Security Team der Var Group, Yarix, hat die Cyberangriffe auf deutsche Unternehmen und Organisationen aus dem Jahr 2024 analysiert. In einem erstmalig veröffentlichten Bericht, dem „Länderbericht zur Cyberbedrohungslandschaft: Deutschland“, stellt Var Group die Ergebnisse vor: Demnach wurden deutsche Unternehmen und Organisationen 2024 vor allem Opfer von Distributed Denial of Service (DDoS) und Web-Defacement sowie Ransomware-Angriffen. Besonders betroffene Branchen waren die Fertigungsindustrie, der Einzelhandel und E-Commerce sowie Regierungseinrichtungen und Strafverfolgungsbehörden.

Die Analyse führte das Yarix Cyber Threat Intelligence (Yarix CTI) Team durch, das Teil von Yarix, dem Kompetenzzentrum für Cybersicherheit der Var Group ist. Grundlage sind vom 1. Januar bis 31. Dezember 2024 registrierte Cyber-Ereignisse, die sich gegen Unternehmen, Einrichtungen und Organisationen mit Sitz in Deutschland richteten. Dafür sammelte das Yarix CTI-Team Threat Intelligence Daten aus offenen Quellen (OSINT) sowie aus geschlossenen Quellen (CLOSINT), beispielsweise aus Untergrund-Cybercrime-Communities und verdeckten Ermittlungen von Threat Intelligence Analysten.

Die Ergebnisse der Analyse inklusive detaillierter Statistiken, Beschreibungen, Einordnungen und Hintergründe zur Bedrohungslage sowie Hypothesen zu möglichen Risikoszenarien in Deutschland für das Jahr 2025 wurden im „Länderbericht zur Cyberbedrohungslandschaft: Deutschland” für 2024 zusammengefasst, der ab sofort unter www.vargroup.de/CTI-Report-DE zum Download zur Verfügung steht.

DDoS/Web-Defacement und Ransomware-Angriffe sind die größte Bedrohung

Das Yarix CTI-Team ordnete die beobachteten Angriffe im Rahmen seiner Analyse sechs Hauptkategorien zu: Die meisten (36,4 Prozent) entfielen auf DDoS und Web-Defacement (siehe Infobox). Auch Ransomware-Angriffe waren für deutsche Unternehmen und Organisationen 2024 ein großes Problem: 27,7 Prozent der beobachteten Attacken lassen sich dieser Kategorie zuordnen. Die 2024 gegen Unternehmen in Deutschland geltend gemachten Ransomware-Angriffe machten unter den 118 analysierten Ländern 2,88 Prozent aller vom Yarix CTI-Team erfassten Ereignisse dieser Art aus. Damit war Deutschland 2024 unter den Top 5-Ländern, die am stärksten von Ransomware-Ereignissen betroffenen waren. Die weiteren Bedrohungen im Beobachtungszeitraum entfielen auf Datenlecks (14,6 Prozent), die Bedrohung durch Leads (8,3 Prozent), unbefugte Zugriffe (8,1 Prozent) und Initial Access Broker (4,9 Prozent).

Das Yarix CTI-Team identifizierte zudem insgesamt 24 Branchen in Deutschland, die 2024 von Cyberangriffen betroffen waren. Ganz oben auf der Liste stehen mit 13,1 Prozent der beobachteten Angriffe die Fertigungsindustrie, dahinter Einzelhandel und E-Commerce (12,2 Prozent) sowie Regierung, Verwaltung und Strafverfolgung (11,8 Prozent). Danach folgen Angriffe auf sektorübergreifende Unternehmen (7,9 Prozent), Verkehr (6,9 Prozent), Consulting (5,5 Prozent), IT (5,3 Prozent), Nachrichten, Medien und Blogs (5,1 Prozent), Finanzen (5,1 Prozent) sowie Energie (4,5 Prozent).

„Häufig Websites staatlicher Institutionen angegriffen“

Die Unternehmen und Organisationen der aufgeführten Branchen hatten aber nicht mit Angriffen aller Bedrohungskategorien gleichermaßen zu kämpfen. Die Bedrohung durch DDoS und Web-Defacement betraf demnach besonders häufig (mit 29,1 Prozent) Regierungs-, Verwaltungs- und Strafverfolgungsbehörden. „Solche Attacken werden häufig von hacktivistischen Gruppen – also Hackergruppen, die ihre Angriffe mit politischen, gesellschaftlichen oder ideologischen Motiven durchführen – durchgeführt“, erklärt Hartmut Mersch, Geschäftsführer von Yarix auf dem DACH-Markt. Ziel von hacktivistischen Gruppen ist es, gesellschaftliche Konflikte zu befeuern und gegen die innen- oder außenpolitische Agenda einer Regierung zu protestieren. „Mit DDoS- und Web-Defacement-Angriffen werden deshalb häufig Websites staatlicher Institutionen angegriffen, um diese lahmzulegen oder auf ihnen Falschinformationen zu verbreiten“, führt Mersch aus. Weitere besonders von DDoS/Web-Defacemente betroffene Branchen waren Verkehr (12,8 Prozent) und die Fertigungsindustrie (10,1 Prozent).

Deutsche Fertigungsindustrie im Fokus von Ransomware-Attacken

Ransomware-Angriffe betrafen mit Abstand am stärksten die Fertigungsindustrie (30,2 Prozent). Dahinter folgen Consulting (11,8 Prozent), IT (8,1 Prozent) und das Baugewerbe (8,1 Prozent). „Im produzierenden Gewerbe haben schon kurze Ausfälle der IT enorme Folgen, beispielweise wenn deswegen eine Produktionskette ausfällt. Jede Minute kostet hohe Summen, weshalb Unternehmen schnell bereit sind, das Lösegeld zu bezahlen,“ erklärt Mersch. „Das macht die produzierende Industrie zu einem beliebten Ziel unter Cyberkriminellen.“

Mit Ransomware-Angriffen hatten zudem vor allem kleine Unternehmen mit 11 bis 100 Mitarbeitenden (55,2 Prozent) zu kämpfen. An zweiter Stelle folgen mittlere Unternehmen mit 101 bis 500 Mitarbeitenden (25,0 Prozent), an dritter Stelle „Enterprise“-Unternehmen mit mehr als 1001 Mitarbeitenden (11,1 Prozent). „In vielen kleinen Unternehmen hat die IT im Vergleich zu großen Unternehmen keinen so hohen Stellenwert. Zudem ist das Mitarbeiterwissen um IT-Sicherheit häufig nicht ausreichend. Das macht sie besonders anfällig“, erläutert Mersch. Das Verständnis des Ausmaßes von Cyberattacken, insbesondere Ransomware, ist selten vorhanden. Deswegen beschäftigen sie sich eher reaktionär als präventiv mit dem Thema Cybersicherheit. „Bei kleinen Unternehmen ist das allerdings besonders tragisch, da diese nicht die Budgets für Absicherungen oder professionelle Incident Response haben“, berichtet Mersch weiter.

Spitze der Cyberangriffe im November und Dezember

Mit Blick auf die Zeitachse der im Jahresverlauf insgesamt registrierten Angriffe stellte das YCTI-Team eine schwankende Verteilung der beobachteten Bedrohungen über die meisten Monate des Jahres mit einer deutlichen Spitze im November und Dezember 2024 fest. DDoS- und Web-Defacement-Angriffe konzentrierten sich auf bestimmte Monate, die mit außenpolitischen Initiativen der deutschen Regierung im geopolitischen Kontext des Jahres 2024 korrespondieren. Dazu zählen beispielsweise die Unterstützung für die Ukraine und Israel. Darüber hinaus wurden auch während wichtiger innenpolitischer Ereignisse und Proteste, etwa den Protesten der deutschen Landwirte im Januar, Spitzenwerte bei solchen Angriffen verzeichnet.

Ein weiterer Grund für den Anstieg am Ende des Jahres ist die umsatzstarke Phase von Einzelhandel und E-Commerce vor Weihnachten. Mersch führt aus: „Wenn ein Cyberkrimineller einem Online-Shop so richtig schaden möchte, dann greift er in dieser Zeit an – von Black Friday bis Weihnachten."

„Cybersicherheit wird ein wirtschaftlicher Vorteil"

Das Yarix CTI-Team schließt seinen Report für 2024 mit einer Einschätzung zu möglichen Bedrohungsszenarien für die Cybersicherheit in Deutschland im Jahr 2025. Dabei stuft es sowohl das Risiko von DDoS- und Web-Defacement-Angriffen als auch das Risiko von Ransomware-Angriffen gegen deutsche Ziele als hoch ein. „Aus den Ergebnissen lässt sich folgern, dass Cybersicherheit in Zukunft zu einem wirtschaftlichen Vorteil wird", betont Mersch. „Standards und Zertifizierungen, die über die künftigen gesetzlichen Vorgaben wie beispielsweise NIS2 hinausgehen, schaffen Vertrauen bei Kunden – und werden dahingehend Unternehmensentscheidungen beeinflussen." Besonders kleine Unternehmen in der Fertigungsindustrie und im Einzelhandel/E-Commerce sowie Regierungs-, Verwaltungs- und Strafverfolgungsbehörden sollten Cybersicherheit mit hoher Priorität betrachten.

Infobox: Kategorien von Cyberbedrohungen im Bericht

DDOS: Bei einem DDoS-Angriff (Distributed Denial of Service) sendet ein Netzwerk aus vielen kompromittierten Computern gleichzeitig massenhaft Anfragen an einen Server, um ihn zu überlasten. Dadurch wird die betroffene Website oder der Onlinedienst für Nutzer unerreichbar. Mögliche Folgen sind Ausfallzeiten, Umsatzverluste und Reputationsschäden.

Web-Defacement: Unter Web-Defacement wird die unbefugte Veränderung der Homepage oder interner Seiten einer Website verstanden. Das Ziel der Angreifer ist meist die öffentliche Bloßstellung oder die Verbreitung ideologischer Inhalte. Web-Defacement kann zu Serviceunterbrechungen führen und den Ruf des Unternehmens oder der Organisation schädigen.

Ransomware: Hierbei blockiert eine Art Schadsoftware durch Datenverschlüsselung den Zugang zu Computersystemen. Dadurch verlieren Betroffene den Zugriff auf wichtige Dateien oder Betriebsfunktionen. Ziel ist es, vom Opfer ein Lösegeld (engl.: Ransom) zu erpressen, damit der Zugang zu den Systemen wiederhergestellt wird.

Unberechtigter Zugriff: Unbefugter Zugriff auf die Computersysteme einer Organisation, eines Unternehmens oder einer Person – meist mit der Absicht, deren Betrieb zu stören und/oder Daten zu entwenden.

Datenleck: Beschreibt das Entwenden von Daten durch unbefugten Zugriff auf die Computersysteme einer Organisation oder eines Unternehmens.

Leads: Im Cyber-Untergrund beziehen sich Leads auf gestohlene Kundendaten wie personenbezogene Daten, Kreditkartendaten oder Anmeldedaten, um Identitätsdiebstahl, Betrug oder gezielte Phishing-Angriffe durchzuführen. Häufig werden Leads auf Schwarzmärkten geteilt oder verkauft.

IAB (Inital Access Broker): Ein Initial Access Broker (IAB) ist ein Cyberkrimineller, der sich unbefugt Zugang zu Unternehmensnetzwerken verschafft und diesen Zugang anschließend an andere Angreifer – etwa für Ransomware-Angriffe – weiterverkauft.

Über Var Group

Var Group ist ein internationaler Anbieter digitaler Dienstleistungen und IT-Lösungen. Seit mehr als 50 Jahren unterstützt Var Group Unternehmen jeder Größe bei der digitalen Evolution. Dabei liegt der Fokus auf Smart Services, Digital Cloud, Cyber Security, Multimedia Workspaces, Data Science, Digital Experience, Var Industries, Business Application International, Industry Solution Retail & Logistik in der Food-Branche. Als 360° IT-Dienstleister – von Beratung und Strategie über Implementierung bis Service und Wartung – bedient das Unternehmen den industriellen Sektor in Branchen wie Automotive, Maschinenbau, produzierendes Gewerbe, Pharma, Lebensmittel, Textilien, Mode, Luxus und Möbel sowie den Einzelhandel.

Var Group S.p.A. mit Sitz in Empoli (Italien) und einem Jahresumsatz von 823 Mio. Euro ist der italienische Marktführer für Software- und Systemintegrationslösungen und über ihre Muttergesellschaft Sesa an der italienischen Börse notiert. Über 3.850 hochqualifizierte Mitarbeitende in 13 Ländern unterstützen Kunden dabei, sich erfolgreich für den Wettbewerb in der Zukunft aufzustellen. Auf dem deutschen Markt agiert Var Group durch ihre Tochter Var Group GmbH mit Sitz in München.

Als Mitglied des UN Global Compact setzt sich der IT-Spezialist aktiv für Nachhaltigkeit und soziale Gerechtigkeit ein. Var Group verfolgt einen integrativen Ansatz und fördert Individualität, Vielfalt und Chancengleichheit, u. a. mit Programmen zur Förderung von Frauen in der IT-Branche und in Führungspositionen.

Weitere Informationen unter www.vargroup.de

[Bilder und Text zur freien Verwendung]

Bildmaterial

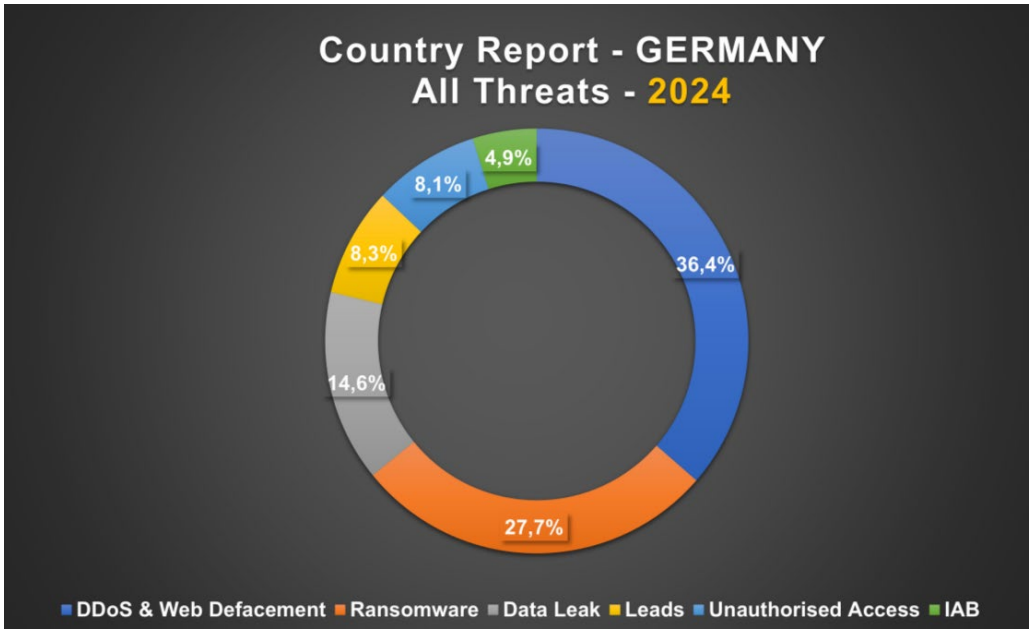
[Var Group_Hartmut_Mersch]

Bildunterschrift: Hartmut Mersch ist seit Mai 2025 Geschäftsführer von Yarix auf dem DACH-Markt. | Foto: Var Group

[Var Group_Länderbericht zur Cyberbedrohungslandschaft-Deutschland_Cover]

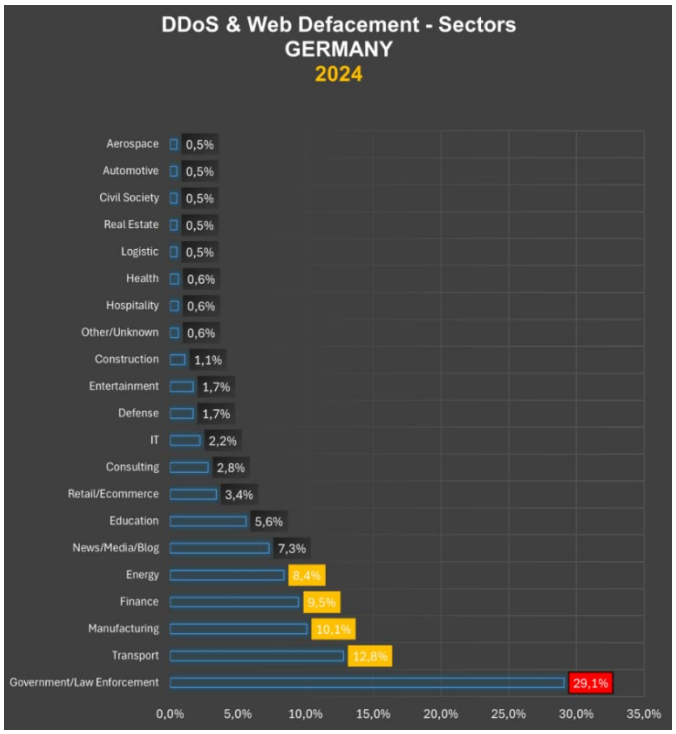
Bildunterschrift: Der Cyber Threat Landscape Country Report für Deutschland liefert wertvolle Einblicke in die aktuelle Bedrohungslage durch Cyberangriffe in Deutschland. | Foto: Var Group

[Var Group_Angriffe nach Bedrohungskategorie]



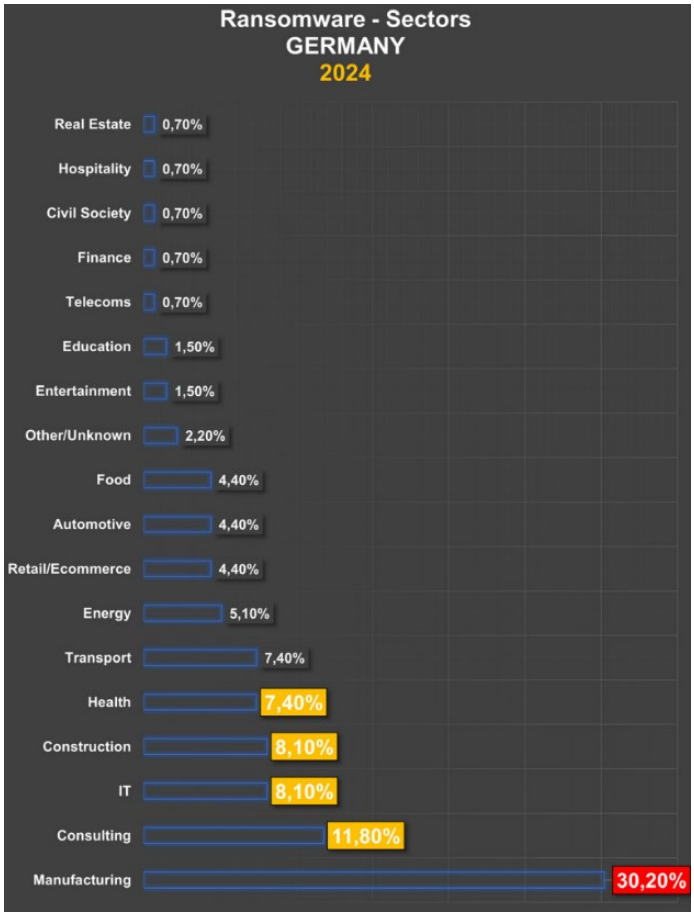
Bildunterschrift: Die meisten Cyberangriffe (36,4 Prozent) entfallen auf DDoS und Web-Defacement.
Bildnachweis: Var Group

[Var Group_DDoS und Web-Defacement nach Branchen]



Bildunterschrift: Mit 29,1 Prozent sind Regierungseinrichtungen, Verwaltungs- und Strafverfolgrungsbehörden am mesiten von DDoS und Web-Defacement betroffen.
Bildnachweis: Var Group

[Var Group_Ransomware-Angriffe nach Branchen]



Bildunterschrift: 30,2 Prozent der beobachteten Ransomware-Angriffe betreffen die Fertigungsindustrie.

Bildnachweis: Var Group

Pressekontakt

Maura Możejko

Carta GmbH
www.carta.eu
Iggelheimer Straße 26
67346 Speyer
Deutschland

Mail: var@carta.eu
Tel.: +49 (0) 6232 / 100 111-13

Unternehmenskontakt

Franziska Unterfrauner

Var Group
www.vargroup.de
Mies-van-der-Rohe-Straße 8
80807 München
Deutschland

Mail: f.unterfrauner@vargroup.com
Tel.: +49 (0) 1512 5021562