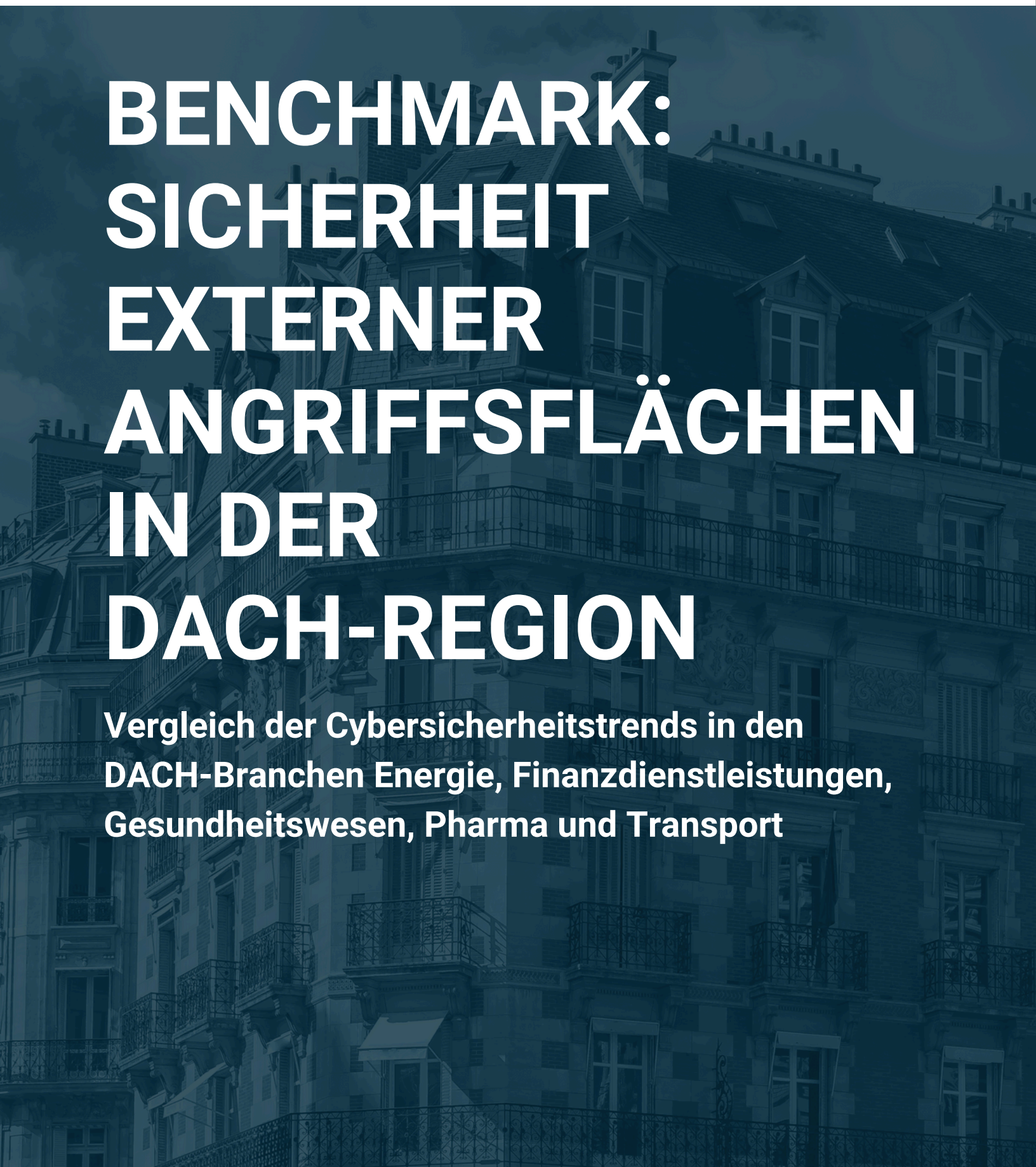
AN OUTPOST24 WHITEPAPER

Outpost24



BENCHMARK: SICHERHEIT EXTERNER ANGRIFFSFLÄCHEN IN DER DACH-REGION

Vergleich der Cybersicherheitstrends in den DACH-Branchen Energie, Finanzdienstleistungen, Gesundheitswesen, Pharma und Transport

Inhalt

Highlights

Über 20.000 Assets analysiert

> 20 % aller Ergebnisse wurden als “kritisches”, “sehr hohes” oder “hohes” Risiko eingestuft.

Der Gesundheitssektor schnitt mit 23,2 % kritischen, sehr hohen oder hohen Schwachstellen am schlechtesten ab.

Known Exploitable Vulnerabilities (KEVs)

54 % der KEVs in der Pharma-Branche wurden als “kritisch” oder “sehr hoch” eingestuft.

Verglichen zum Finanzsektor mit 20,85 %

Geleakte oder gestohlene Zugangsdaten

Gesundheitssektor: Größte Menge an durch Malware gestohlenen Anmeldedaten

Finanzsektor: Die meisten Zugangsdaten, die im Dark Web zum Verkauf angeboten werden

Cookie Consent Violations

Pharma führt die Rangliste an.

Transport und Logistik hat die wenigsten.

Wie wir die Sicherheit der Angriffsfläche in der DACH-Region bewertet haben

Die Bedrohung durch Cyberkriminalität nimmt weltweit zu, und die DACH-Region bildet hier keine Ausnahme. Laut Bitkom-Umfrage "Wirtschaftsschutz 2024" geben 80 % der Befragten an, dass Cyberangriffe in den letzten zwölf Monaten zugenommen haben. Mit einem geschätzten Schaden von 178,6 Milliarden Euro machen Cyberangriffe auch 67 % des Schadens von Angriffen gegen Unternehmen aus. Schätzungen zufolge sind rund 60 % der Unternehmen in der DACH-Region in den letzten zwei Jahren mindestens einem Cyberangriff zum Opfer gefallen. Die deutschen Behörden gaben bekannt, dass sie im Jahr 2023 einen Anstieg der Cyberangriffe aus dem Ausland um 28 % verzeichneten. Daher ist es wichtiger denn je, eine Angriffsfläche zu schaffen, die für potenzielle Hacker nicht besonders attraktiv ist.

Vollkommener Schutz gegen Cyberangriffe ist aber leider unmöglich, und es wird wohl nie der Tag kommen, an dem keine Schwachstellen oder Risiken mehr zu beseitigen sind. Dennoch sollten Unternehmen einen Blick darauf werfen, welche Fortschritte sie bereits in diesem Bereich gemacht haben. Daher ist es interessant zu wissen, wo Sie mit Ihren Bemühungen um die Cybersicherheit im Vergleich zu anderen Unternehmen innerhalb Ihrer Branche stehen. Zu diesem Zweck haben wir mit unserer Lösung für externes Attack Surface Management (EASM) einen „Benchmark“ erstellt, der Aufschluss darüber gibt, wie sich die verschiedenen Angriffsflächen in einigen der größten Branchen in der DACH-Region voneinander unterscheiden.

Für diese Analyse haben wir fünf große Industriezweige in der DACH-Region ausgewählt: Energie, Finanzdienstleistungen, Gesundheitswesen, Pharmaindustrie und Logistik. Aus jeder dieser Branchen haben wir eine Mischung aus („Non-Customer“-)Organisationen ausgewählt, die eine ausgewogene Mischung aus sowohl namhaften Organisationen als auch kleineren Unternehmen darstellt. Anschließend analysierten wir für jedes Unternehmen durchschnittlich zehn Domains, ausgehend von einer primären Domain, der Top-Domain eines Unternehmens (z.B. Outpost24.com). Daraus haben unsere Experten dann die interessantesten Datentrends zusammengestellt.

Wichtig ist dabei, dass die EASM-Lösung von Outpost24 nur öffentlich verfügbare, mit dem Internet verbundene IT-Assets findet und analysiert. Dies geschieht durch die Simulation von normalem Internetverkehr, passiven Erkennungs- und Testverfahren. So kann ein umfassender Einblick in bekannte oder bisher unbekannte Assets eines Unternehmens erhalten werden. Zudem ermöglicht die Simulation es, diese Assets anhand ihres Risikos zu bewerten. Der Prozess ist völlig passiv und analysiert nur öffentlich verfügbare Informationen.

Die Analyse wurde im August 2024 durchgeführt. Da es sich um eine Momentaufnahme handelt, die sich im Laufe der Zeit verändern wird, sind einige Ergebnisse aktuell nicht mehr auf dem gleichen Stand wie zum Zeitpunkt der Analyse. Wir gehen jedoch davon aus, dass die allgemeinen Trends konsistent geblieben sind, und hoffen, Ihnen damit einen wertvollen Überblick über die häufigsten Risiken und Schwachstellen in den Schlüsselindustrien der DACH-Region zu geben.

Zum Schluss zeigen wir Ihnen, wie Sie EASM nutzen können, um die Angriffsfläche Ihres eigenen Unternehmens zu bewerten und herauszufinden, wie Sie im Vergleich zum Branchendurchschnitt abschneiden.

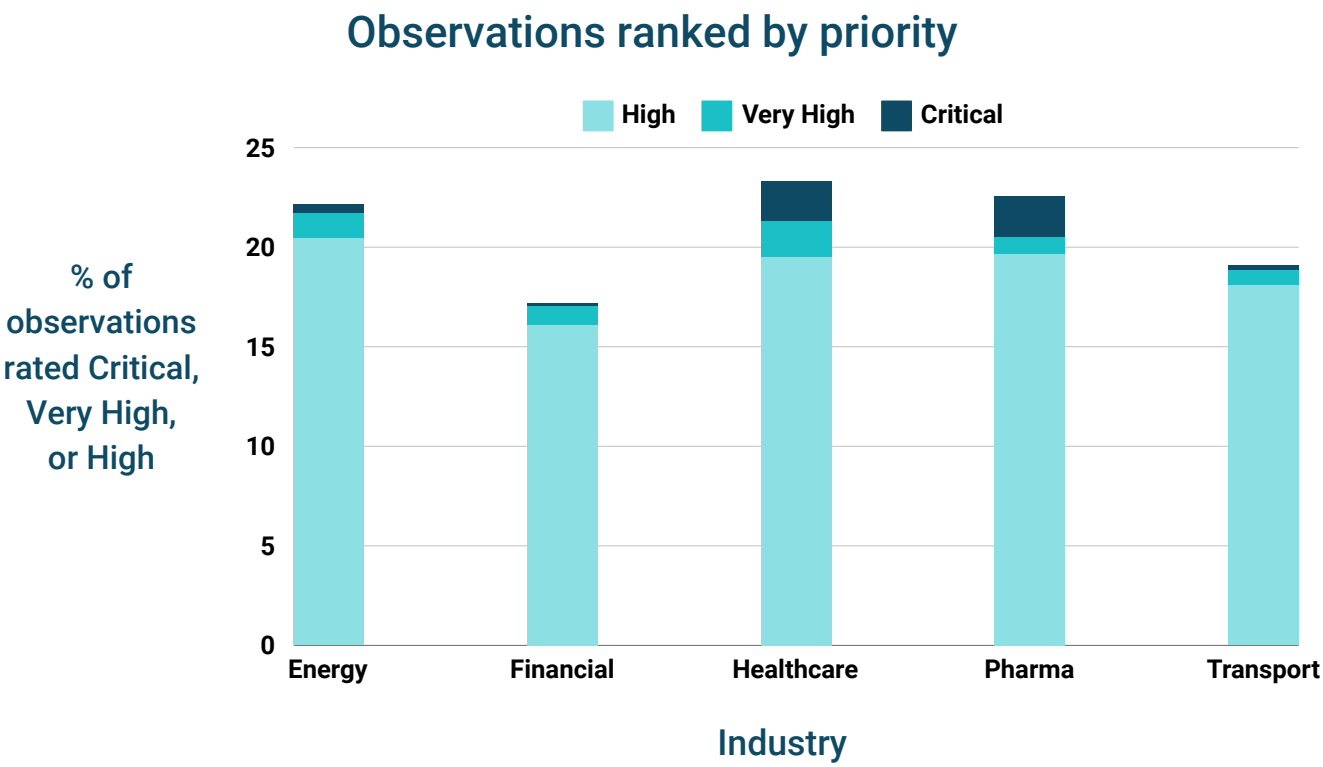
Eine Bewertung der kritischsten Ergebnisse

Für die Benchmarks haben wir ca. 20.000 Assets ausgewertet. Wurde bei einem Asset ein sicherheitsrelevantes Merkmal gefunden, wurde es als „Observation“ eingestuft und je nach Schwere der Gefahr mit einer Punktzahl bewertet. Um den Schweregrad dieser Ergebnisse zu unterscheiden, haben wir ein einfaches Klassifizierungssystem verwendet, das die Gefahren wie folgt einstuft: kritisch, sehr hoch, hoch, mittel, niedrig und sehr niedrig.

Die Angriffsfläche von Unternehmen vergrößert sich ständig und kann bei größeren Organisationen schnell unübersichtlich werden. Das kann dazu führen, dass IT-Sicherheitsteams nicht mehr wissen, wo sie anfangen sollen. Ein wichtiger Bestandteil von EASM ist daher die Möglichkeit, gefundene Gefahren entsprechend zu klassifizieren, um bei Bedarf eine nötige Triage vornehmen zu können. Auch bei dieser Analyse haben wir uns auf die Gefahren konzentriert, die Unternehmen am dringendsten lösen sollten. Wie schnitten also die fünf Branchen in Bezug auf den Prozentsatz der Observationen ab, die als kritisch, sehr hoch und hoch eingestuft wurden?

Die ersten Ergebnisse

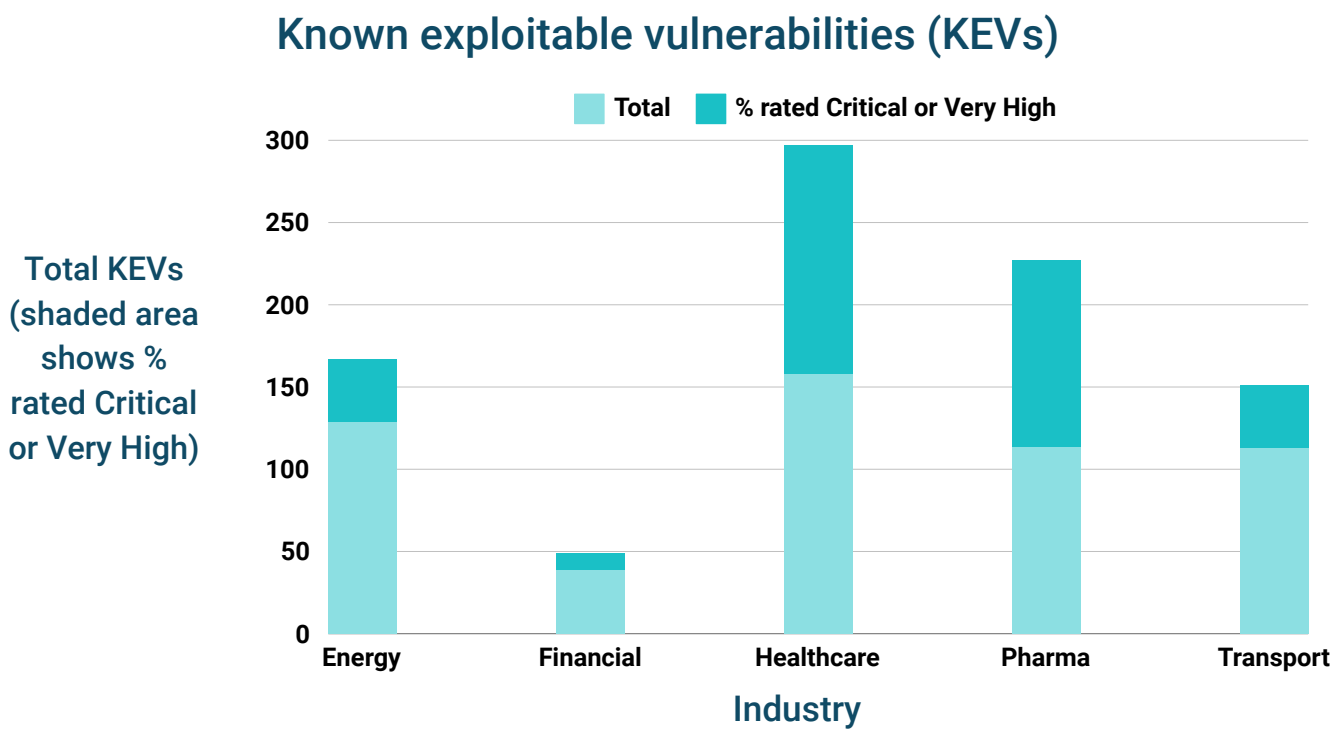
Wie Sie aus dem folgenden Diagramm entnehmen können, wies die Gesundheitsbranche die höchste Anzahl von Beobachtungen (23,21 %) auf, die als kritisch, sehr hoch oder hoch eingestuft wurden. Der Finanzsektor hatte mit 17,21 % den geringsten Anteil an bedenklichen Ergebnissen. Wir gehen davon aus, dass aufgrund der strengen branchenspezifischen Vorschriften die Finanzbranche bereits viele Cybersecurity-Themen angeht, was den großen Unterschied erklären könnte. Dennoch sind über alle Branchen hinweg 20,33 % aller Ergebnisse als kritisch einzustufen, was ein hohes Risikopotenzial für alle untersuchten Branchen in der DACH-Region ausweist.



Auf dieser Grundlage haben wir die Daten weiter aufgeschlüsselt und die Anzahl der sogenannten „known exploited vulnerabilities“ (KEVs) untersucht, die in jeweiligen Angriffsflächen der einzelnen Branchen auftauchen. KEVs sind besonders gefährlich, da wir bereits wissen, dass sie von Angreifern ausgenutzt werden können (und wahrscheinlich auch werden). Da diese Schwachstellen bereits bekannt und dokumentiert sind, sollten Unternehmen bei der Behebung ein besonderes Augenmerk auf diese Schwachstellen legen.

Als Beispiel für eine KEV können wir CVE-2021-40438 anführen, die sich auf einen bekannten Apache-Exploit bezieht. Dennoch wurde diese Schwachstelle in allen untersuchten Branchen gefunden.

Besonders in der Pharmaindustrie sind die Ergebnisse besorgniserregend: Wir konnten 247 KEVs feststellen, von denen 54 % als kritisch oder sehr hoch eingestuft wurden. Das Gesundheitswesen hatte mehr KEVs (297), aber ein kleinerer Anteil davon wurde a ls kritisch oder sehr hoch eingestuft (46,8 %). Auch hier hatte der Finanzsektor in der DACH-Region die Dinge besser unter Kontrolle: Nur 20,85 % der beobachteten KEVs wurden als kritisch oder sehr hoch eingestuft.



Oupost24-Analyse: Warum sehen wir solche großen Unterschiede zwischen den einzelnen Branchen?

Die Branchen unterscheiden sich hinsichtlich ihrer Attraktivität für Angreifer. So ist beispielsweise jeder Sektor, der große Mengen sensibler und personenbezogener Daten (Adressen, Sozialversicherungsnummern, Gesundheitsdaten usw.) verarbeitet, ein attraktives Ziel für Hacker, die damit Identitätsdiebstahl begehen oder sie an andere Bedrohungsakteure weiterverkaufen können. Zudem gibt es in den einzelnen Branchen unterschiedlich strenge Vorschriften und Standards im Bezug auf Cybersecurity, Awareness und Compliance.

Doch nicht nur Standards und Vorschriften variieren, sondern auch die Finanzierung von Personal und Technologien im Bereich der Cybersicherheit. In diesem Datensatz zeigte sich, dass der Finanzsektor die geringste Anzahl von kritischen, sehr hohen und hohen Beobachtungen aufwies. Derselbe Trend war bei den KEVs zu beobachten. Möglicherweise spielen hier strenge Vorschriften, mehr Geld, das für die Cybersicherheit zur Verfügung steht, und gravierendere Konsequenzen im Falle eines erfolgreichen Angriffes eine Rolle.

Im Gegensatz dazu schneidet der Gesundheitssektor schlecht ab, was vielleicht daran liegt, dass diese Branche bereits stark unter Druck steht. Alte Systeme, weniger technisches Personal, kleinere Budgets und auch weniger Fokus auf Cybersecurity in der Lieferkette und in den eingesetzten Systemen können mögliche Gründe sein. Letztendlich müssen auch die Mitarbeiter schnell und einfach auf die Systeme zugreifen können, was nicht immer mit den Best Practices übereinstimmt. Leider führt dies zu einer Umgebung, in der Schwachstellen gedeihen können, und macht sie zu einem attraktiven Ziel für Angreifer.

Geleakte und gestohlene Zugangsdaten

Gestohlene oder kompromittierte Zugangsdaten sind weiterhin ein beliebtes Einfallstor für Cyberkriminelle, um Zugriff auf vertrauliche Daten zu erhalten. Im Rahmen dieser Analyse kommt die Integration der Bedrohungsinformationen des Threat Intelligence(IT)-Teams von Outpost24 zum Einsatz. Damit können Unternehmen untersuchen, ob Zugangsdaten von Nutzern, die im Zusammenhang mit den analysierten Domains stehen, gestohlen wurden. Für eine bessere Übersicht unterteilt die EASM-Lösung die Ergebnisse in zwei verschiedene Kategorien: durch Malware gestohlene Daten und Dark Web-Quellen.

Bei Zugangsdaten, die durch Malware gestohlen wurden, kann es sein, dass der betroffene Endbenutzer die Malware versehentlich heruntergeladen, eine damit infizierte Website auf seinem Arbeitsgerät genutzt oder dass er seine Zugangsdaten für die Arbeit auf einem mit Malware infizierten privaten Gerät verwendet hat. Dark Web bedeutet, dass das TI-Team die Daten in Untergrundforen oder Marktplätzen gefunden hat und sie dort zum Verkauf stehen.

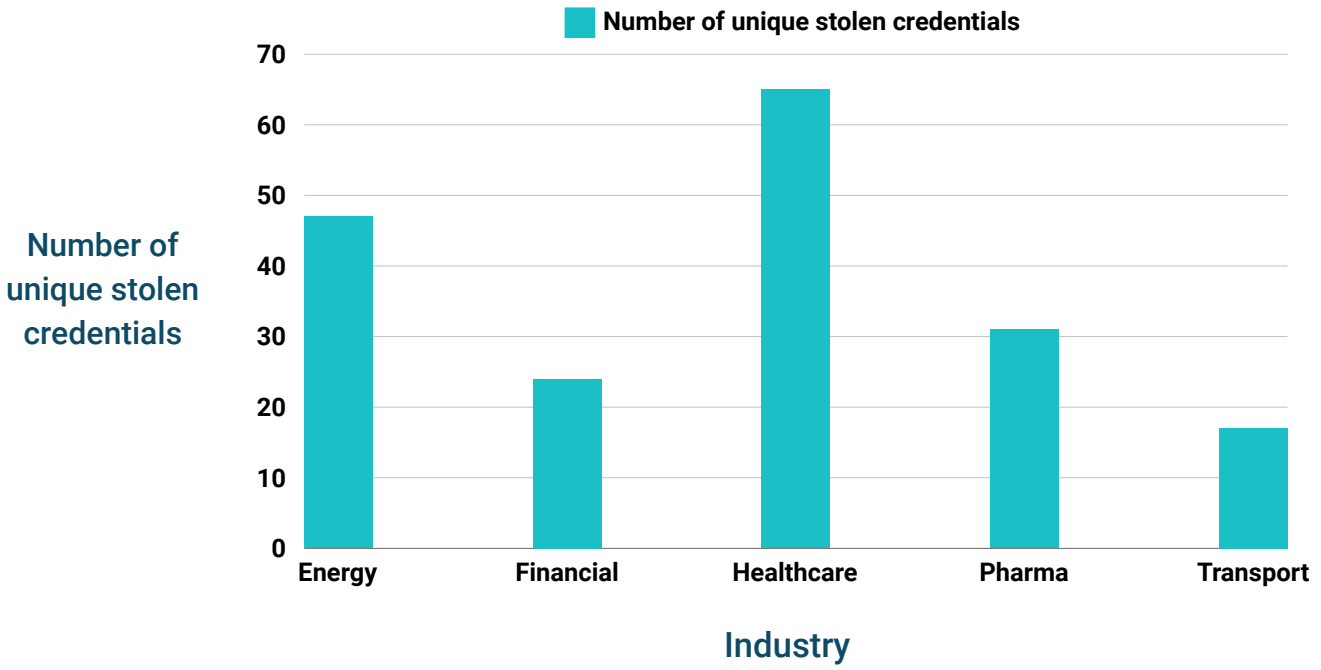
Kompromittierte Zugangsdaten in den Branchen

Interessanterweise verzeichneten wir die zweitwenigsten durch Malware gestohlenen Zugangsdaten im Finanzsektor, aber die höchste Anzahl von Zugangsdaten, die im Dark Web verkauft wurden. Dies könnte darauf hindeuten, dass Unternehmen in der Finanzbranche in Cybersicherheitsmaßnahmen investiert haben, die Malware gut abwehren, aber auch darauf, dass die Anmeldedaten ihrer Endnutzer im Dark Web bei Initial Access-Brokern sehr begehrt sind.

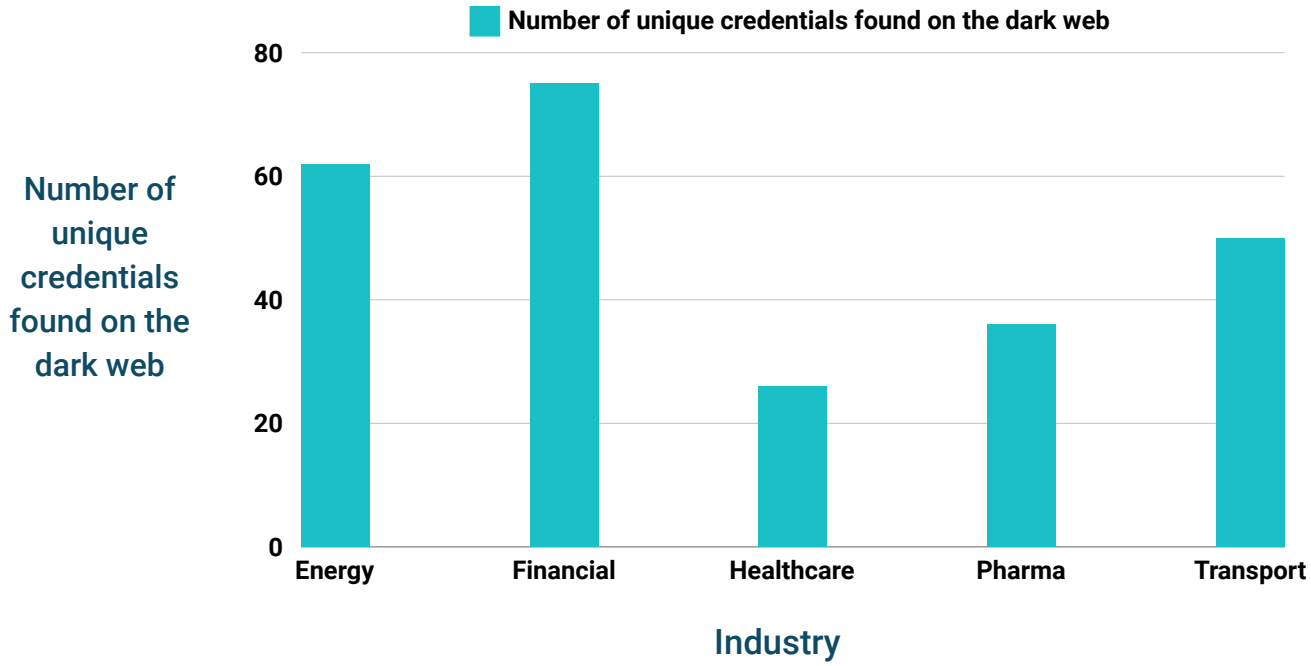
Das verdeutlicht auch, dass Hacker mehrere Wege beschreiten können, wenn sie bestimmte Branchen ins Visier nehmen wollen. Während Unternehmen vielleicht einen Bereich gut unter Kontrolle haben, können sie in anderen Bereichen verwundbar sein, oder es fehlt ihnen an Transparenz bei spezifischen Problemen.

Denn wenn ein Angriffsweg blockiert ist, werden Hacker nach alternativen Möglichkeiten suchen, um an Zugangsdaten zu gelangen.

Malware-stolen credentials



Credentials on the dark web



Oupost24-Analyse: Warum die Jagd nach kompromittierten Zugangsdaten weiterhin wichtig ist

Für die meisten Unternehmen sind Passwörter das schwächste Glied und eines der einfachsten Einfallstore für Angreifer. Warum sich mühsam einhacken, wenn man sich einfach anmelden kann? Laut dem Data Breach Investigations Report 2024 von Verizon lassen sich 31 % aller Cyberangriffe und Datenschutzverletzungen auf kompromittierte Zugangsinformationen zurückverfolgen. Um weitere Angriffe dieser Art zu verhindern, ist es wichtig, dass Sie wissen, ob Zugangsdaten aus Ihrem Unternehmen bereits in die falschen Hände gelangt sind.

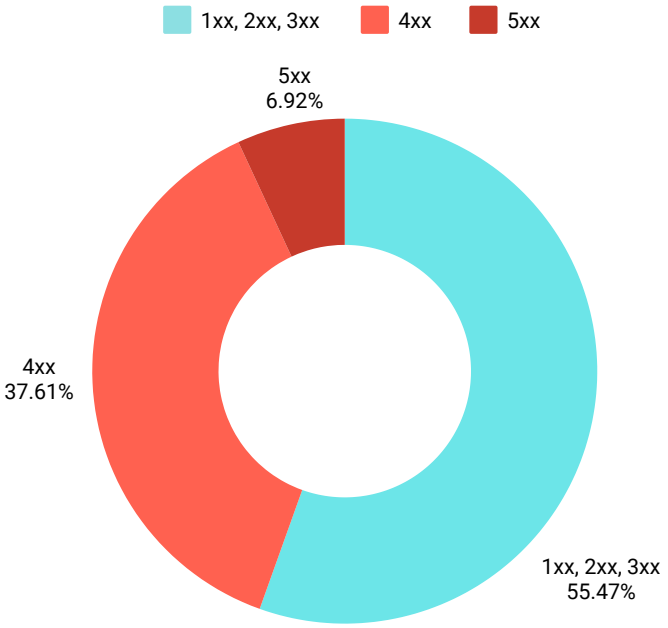
Cyber-Hygiene und Verschlüsselung

Wenn wir von „Cyber-Hygiene“ sprechen, meinen wir Bemühungen, die grundlegende Funktionsfähigkeit und Sicherheit von Hardware und Software aufrechtzuerhalten – wie zum Beispiel den Umgang mit Webserver-Fehlercodes. HTTP-Statuscodes klassifizieren die Antworten des Servers auf die Anfrage des Browsers. Manchmal führt eine Anfrage zu einer Fehlermeldung, wenn ein Benutzer versucht, über einen Browser zu interagieren – „404 page not found“ ist die übliche Meldung, die jeder kennt. Alle HTTP-Antwortstatuscodes werden in fünf Kategorien eingeteilt, die wie folgt definiert sind:

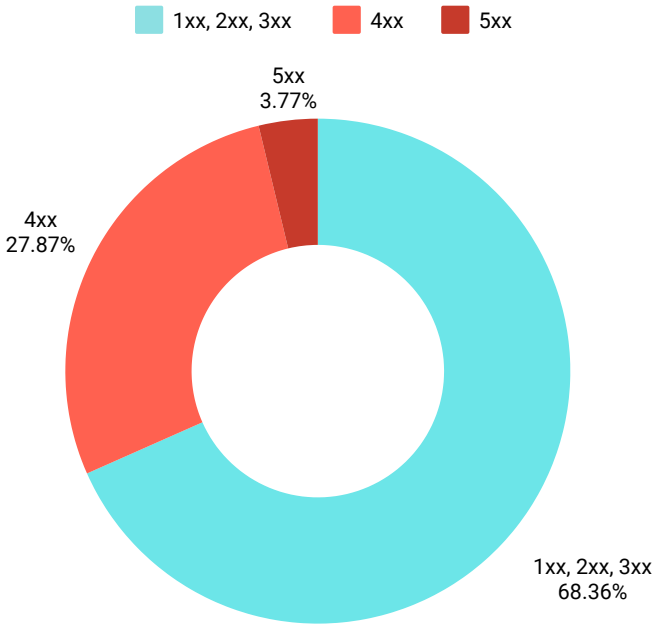
- 1xx informational response – die Anfrage wurde empfangen, der Prozess wird fortgesetzt;
- 2xx erfolgreich – die Anfrage wurde erfolgreich empfangen, verstanden und akzeptiert;
- 3xx redirection – es müssen weitere Maßnahmen ergriffen werden, um die Anfrage abzuschließen;
- 4xx client error – die Anfrage enthält eine fehlerhafte Syntax oder kann nicht erfüllt werden;
- 5xx server error – der Server konnte eine scheinbar gültige Anfrage nicht beantworten.

Die Behebung von 4xx- und 5xx-Fehlern sollte ein Quick-Win für Unternehmen sein, vorausgesetzt, sie kennen die Ursachen für die Fehler. Wie Sie aus den unten stehenden Diagrammen ablesen können, gibt es dennoch in allen DACH-Branchen Potenzial für eine Optimierung der digitalen Prozesse. Insbesondere die Pharmaindustrie hatte eine sehr hohe Anzahl von 4xx-Client-Errors, wohingegen der Finanzsektor die wenigsten Fehler aufwies.

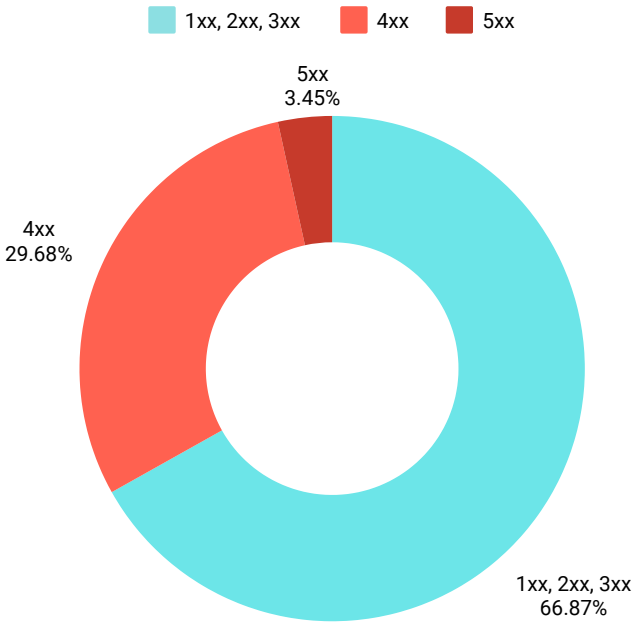
Energy



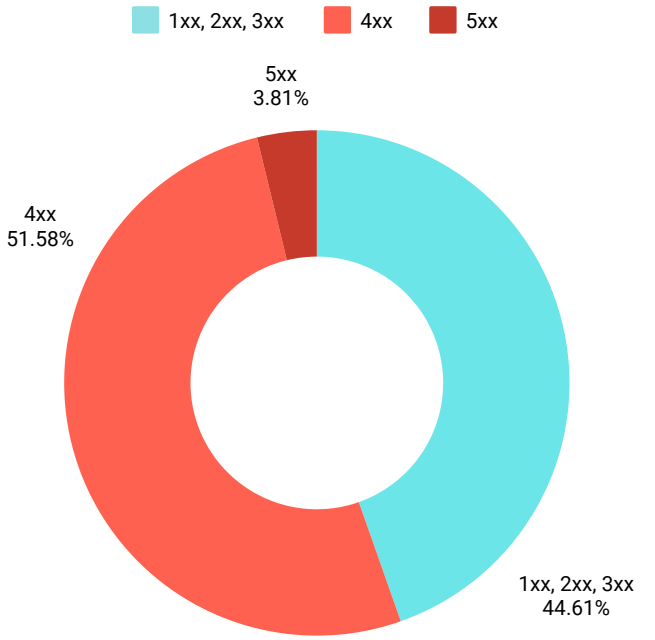
Financial

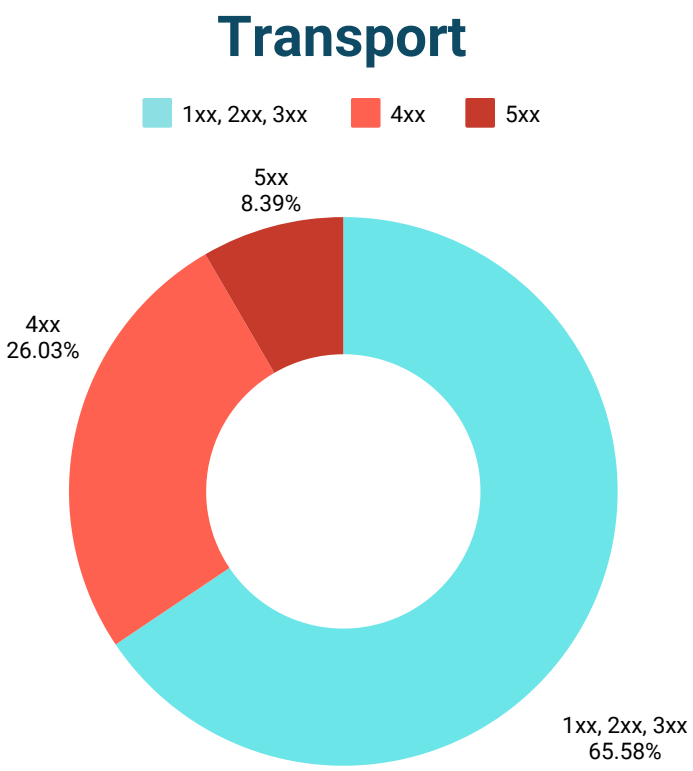


Healthcare



Pharma

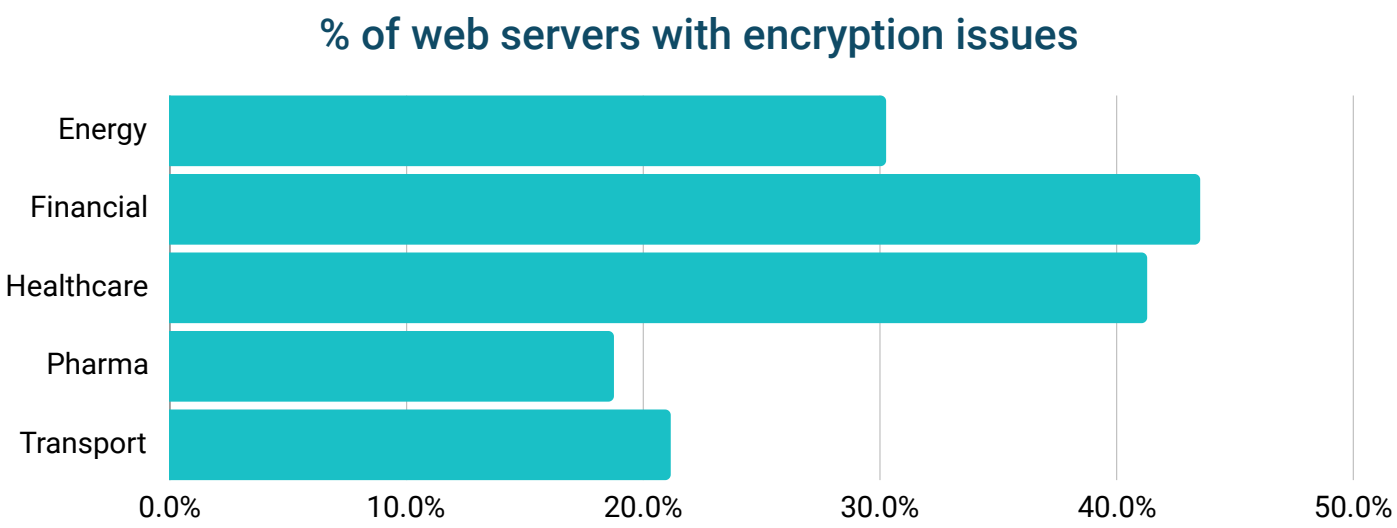




Verschlüsselung von Webtraffic

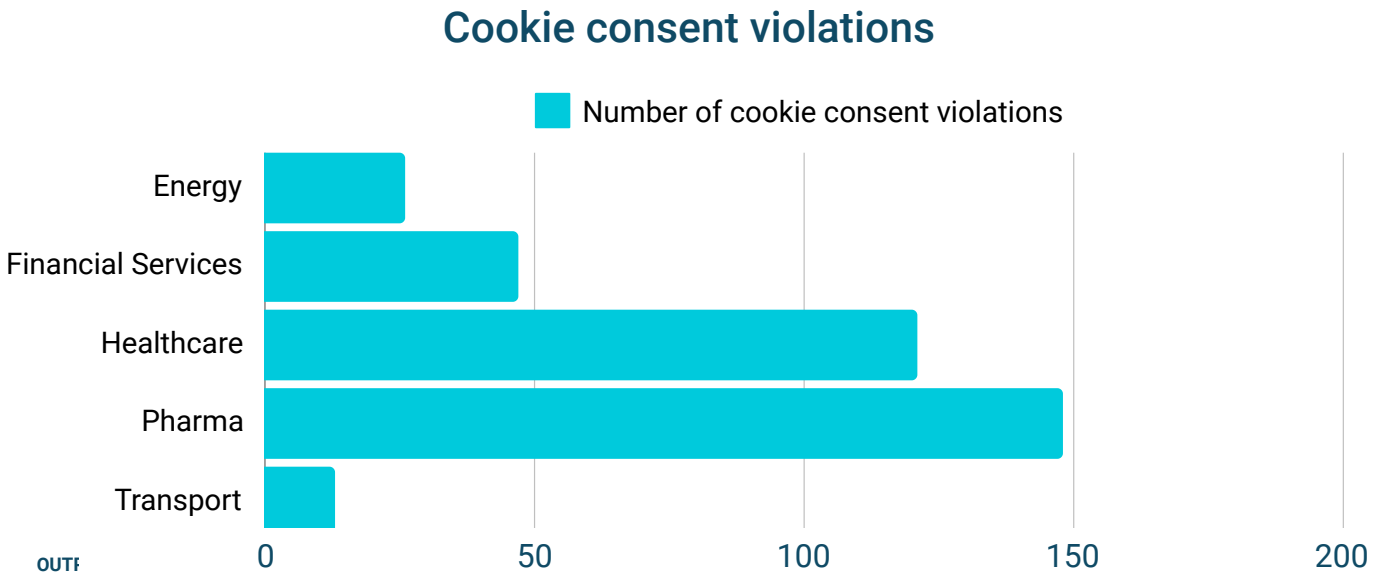
ISSL/TLS-Zertifikate sind digitale Zertifikate, die die Identität einer Website authentifizieren und eine verschlüsselte Verbindung ermöglichen. Fehlkonfigurationen bei diesen Zertifikaten gehören zu den häufigsten Problemen, die wir bei einer Analyse der Angriffsfläche feststellen. Zu diesen Fehlern können veraltete Verschlüsselungsalgorithmen, falsche Zertifikatseinstellungen und abgelaufene SSL/TLS-Zertifikate gehören. Wenn sie nicht ordnungsgemäß eingerichtet oder verwaltet werden, können sie zu Schwachstellen im Netzwerk Ihres Unternehmens führen und mögliche Zugangswege für Hacker via Phishing und Man-in-the-Middle-Angriffe eröffnen.

Die Verwaltung des Lebenszyklus dieser Zertifikate kann leicht in Vergessenheit geraten und ist ein häufig unterschätztes Problem. Abgelaufene oder ungültige Website-Zertifikate können für Benutzer abschreckend wirken und für Cyberkriminelle ein Angriffssignal darstellen. Organisationen aus dem Finanzsektor haben bisher in den meisten Kategorien am besten abgeschnitten, sind aber hier die schlimmsten Übeltäter: Bei 43,53 % ihrer Webserver wurden Probleme mit der Verschlüsselung festgestellt.



Cookie Consent Violation

Cookies helfen dabei, das Nutzerverhalten zu analysieren, aber es gibt seit einiger Zeit eine Reihe von Gesetzen und Vorschriften, wie Unternehmen sie einsetzen dürfen. Laut DSGVO darf eine Website nur dann personenbezogene Daten von Nutzern erheben, wenn diese ihre ausdrückliche Zustimmung zu den spezifischen Zwecken ihrer Verwendung gegeben haben. Die Zustimmung der Endnutzer zu Cookies ist die am häufigsten genutzte Rechtsgrundlage der DSGVO, so dass eine hohe Zahl von Verstößen ein potenzielles Risiko darstellt. Am besorgniserregendsten waren die Ergebnisse für die pharmazeutische Industrie, wo 121 Verstöße festgestellt wurden. Im Logistiksektor gab es mit nur 13 die wenigsten.



Oupost24-Analyse: Warum ist Cyber-Hygiene wichtig?

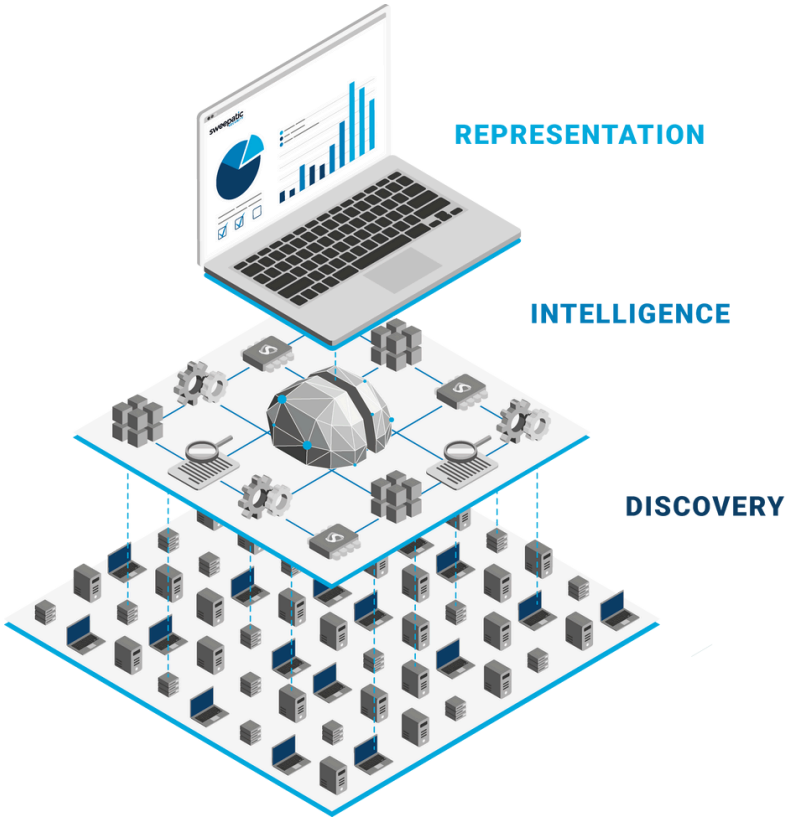
Obwohl mangelnde Cyber-Hygiene nicht automatisch eine Gefahr für kritische Unternehmensdaten darstellt, zeigt sie doch deutlich, dass grundlegende Prozesse nicht reibungslos ablaufen. Für Angreifer sind dies Indizien dafür, dass ein Unternehmen einen Angriff wert sein könnte. Wenn es schon bei SSL-Zertifikaten hapert, dann könnte es vielleicht auch bei anderen Cybersecurity-Maßnahmen lohnenswert sein, etwas tiefer zu bohren. Zudem beeinträchtigen sie auch die Darstellung der Organisation nach außen. Ein Verstoß gegen DSGVO-Anforderungen kann besonders hohe, finanzielle Konsequenzen haben. Daher ist ein EASM-Tool, das solche Mängel aufzeigt, für Organisationen von großer Bedeutung.

External Attack Surface Management in Ihrer Organisation

Im Gegensatz zum klassischen Schwachstellenmanagement, bei dem bereits bekannte Assets bewertet werden, haben wir festgestellt, dass bis zu 30 % der online erreichbaren Assets eines Unternehmens dem Sicherheitsteam nicht bekannt sind. Aus diesem Grund wird EASM eingesetzt, um einen vollständigen Überblick über alle öffentlichen, dem Internet ausgesetzten Assets zu erhalten. So wird verhindert, dass diese von Angreifern ausgenutzt werden. Eine EASM-Lösung bietet IT-Experten Zugang zu einer fortlaufenden Bestandsermittlung sowie zu einer kontinuierlichen Analyse und Überwachung von Änderungen an der Angriffsfläche der Organisation.

Wie EASM funktioniert

Man kann sich EASM als eine Lösung vorstellen, die auf drei Ebenen arbeitet. Zunächst gibt es die Erfassungsebene, auf der Informationen über alle öffentlich zugänglichen Ressourcen im Zusammenhang mit den Domänen Ihres Unternehmens gesammelt werden. Als Nächstes werden die Informationen aus der Erfassungsebene an die Informationsebene weitergeleitet, wo die Angriffsfläche analysiert und Informationen gesammelt werden. Schließlich werden die Daten in einer benutzerfreundlichen und interaktiven Präsentationsebene angezeigt – dem Portal, in dem Sie Schwachstellen finden und mit dem Beheben beginnen können. Die API kann auch mit vielen externen Systemen vernetzt werden.



So hilft Ihnen EASM

Ein wichtiger Aspekt von EASM ist, dass es kontinuierlich und automatisch erfolgt. Eine Angriffsfläche wächst ständig, daher sind Momentaufnahmen nicht gut genug, um sich ein zuverlässiges Bild über die Sicherheitslage Ihrer Organisation zu machen. Sie sollten dauerhaft Ihre unbekannten Schwachstellen aufdecken, bevor Hacker es tun. Das bedeutet, dass Ihre Sicherheitsteams immer den Finger am Puls der Zeit haben müssen, um eine genaue und frühzeitige Warnung zu bekommen. Jedes Unternehmen ist anders, aber es gibt keins, das nicht davon profitieren könnte, einen kontinuierlichen Überblick über seine Online-Assets zu erhalten.

EASM hilft Sicherheitsteams auch dabei, Prioritäten zu setzen und sich auf die wichtigsten Probleme zu konzentrieren. Das bedeutet natürlich nicht, dass man den Rest der Probleme ignoriert, sondern nur, dass man sich zuerst um die potenziell schädlichsten kümmert. Eine Lösung, die diese potenziellen Risiken fortlaufend automatisch bewertet oder priorisiert, ist von entscheidender Bedeutung, damit die Sicherheitsteams nicht zu viel Zeit in diese manuelle Arbeit investieren müssen.

Wie schlägt sich Ihre Angriffsfläche im Vergleich?

Vergleichen Sie, wie Ihre eigene Angriffsfläche im Vergleich zu den Benchmarks der DACH-Branchen abschneidet. Fordern Sie noch heute eine erste Analyse Ihrer Angriffsfläche an, um Bereiche zu identifizieren, in denen Ihre Cybersicherheit stark ist; aber auch Bereiche, in denen Sie Schwachstellen beheben müssen.

Erhalten Sie jetzt einen ersten Einblick in die Sicherheitslage Ihrer Angriffsfläche!

Disclaimer

Diese Analyse wurde extern von Outpost24 unter Verwendung der firmeneigenen EASM-Plattform (External Attack Surface Management), Sweepatic, durchgeführt. Das EASM von Outpost24 findet und analysiert öffentliche IT-Ressourcen, die mit dem Internet verbunden sind, indem es normalen Internetverkehr, passive Erkennung und Testverfahren simuliert. Outpost24 ist nicht mit der Infrastruktur oder den Geschäftsprozessen der Organisationen verbunden, die Gegenstand dieser Analyse sind.

Über Outpost24

Die Outpost24-Gruppe ist Vorreiter im Cyber Risk Management mit Angeboten in den Bereichen Vulnerability Management, Application Security Testing, Threat Intelligence und Access Management.
Über 2.500 Kunden in mehr als 65 Ländern vertrauen auf die Lösungen von Outpost24, um Schwachstellen zu identifizieren, externe Bedrohungen zu überwachen und die Angriffsfläche ihrer Organisationen schnell und zuverlässig zu minimieren.

STANDORTE

GLOBAL HEADQUARTERS SWEDEN
Blekingegatan 1,
371 57 Karlskrona

Email info@outpost24.com

UNITED STATES HEADQUARTERS
123 S Broad St Suite 2530,
Philadelphia, PA 19109

Tel +1 877 773 267

SWEDEN
Vasagatan 7A,
111 20 Stockholm

info@outpost24.com

DENMARK
Axel Towers 2F, 4th floor,
1609 Copenhagen V

Tel +45 53 73 05 67

FRANCE
291 Rue Albert Caquot 06560
Valbonne, Antibes

UNITED KINGDOM
19 Eastbourne Terrace,
London W2 6AA

Poseidon House,
Neptune Park,
Plymouth PL4 0SJ

Tel +44 20 3735 4986

NETHERLANDS
Stadhouderskade 14J,
1054 ES Amsterdam

Tel +31 20 420 9560

BELGIUM
Ubicenter Gebouw A, Philipssite 5/bus 17,
3001 Leuven

Tel +32 16 22 76 60

SPAIN
Plaça de Gal·la Placídia,
1-3, Oficina 303,
08006 Barcelona

Tel +34 933 09 61 00

UNITED STATES 35 S
Washington St., Suite 308,
Naperville, Chicago, IL 60540

Tel +1 877 773 2677

CANADA
517 Wellington Street West,
Suite 400,
Toronto, ON M5V 1G1

Tel +1 877 773 2677

GERMANY
Gierkezeile 12,
10585 Berlin

Tel +49 30166 37218

Outpost24