DBIR 2022: Bergbau-, Öl- und Gasindustrie plus Versorgungsbetriebe

(NAICS 21 und 22)

Herzlich willkommen zum Überblick über die Sektoren Berg- und Tagebau, Öl und Gas sowie die Versorgungsbranche, Ihrer branchenspezifischen Kurzfassung der 15. Ausgabe des jährlich erscheinenden Verizon Data Breach Investigations Report (DBIR). Es ist kaum zu glauben, dass unser erster Bericht nun schon 15 Jahre zurückliegt.

Seither untersuchen wir im DBIR, welche Arten von Cyberangriffen aktuell besonders häufig auftreten und wie Unternehmen sich vor ihnen schützen können. Dieses Jahr haben wir dazu 23.896 Vorfälle analysiert, darunter 403 aus den oben genannten Branchen. Bei 179 dieser Vorfälle wurden den Angaben der Betroffenen zufolge Daten gestohlen. Diese und alle anderen in diesem Bericht präsentierten Zahlen stammen zum einen aus dem Verizon Threat Research Advisory Center (VTRAC), zum anderen von 87 beteiligten Unternehmen und Organisationen aus aller Welt, ohne deren Unterstützung die Erstellung dieser Publikation nicht möglich gewesen wäre.

Wir hoffen, dass Ihnen unser Bericht einen informativen Überblick über die gängigsten Angriffsmethoden in Ihrer Branche sowie nützliche Informationen zur besseren Vorbereitung auf deren Abwehr vermittelt.

Im Folgenden finden Sie eine Übersicht über die für die Branchen Berg- und Tagebau, Öl und Gas sowie Versorgungsunternehmen relevantesten Untersuchungsergebnisse aus dem diesjährigen Bericht, die Sie gern an Ihre Kollegen weiterleiten können. Der vollständige Bericht ist (auf Englisch) unter verizon.com/dbir zum Download verfügbar und enthält eine detailliertere Beschreibung der Bedrohungslage im Jahr 2022.

Im Rahmen unserer DBIR-Berichte nutzen wir das nordamerikanische Branchenklassifizierungssystem NAICS, um die betroffenen Unternehmen und Institutionen Branchen zuzuordnen. NAICS nutzt zwei- bis sechsstellige Codes, um Unternehmen und Organisationen zu klassifizieren. Unsere Analysen finden in der Regel auf der zweistelligen Ebene statt und wir nennen die NAICS-Codes gemeinsam mit der Branchenbezeichnung. Ausführliche Informationen über die Codes und das Klassifizierungssystem finden Sie unter: census.gov/naics/?58967?yearbck=2012

Angriffs- und Vorfallsmuster

Die Angriffs- und Vorfallsmuster wurden im DBIR 2014 als nützliche Typologie häufig auftretender Szenarien eingeführt. Im vergangenen Jahr haben wir sie überarbeitet und ihre Anzahl von neun auf acht reduziert, um Veränderungen in den Angriffsmethoden und der Bedrohungslage widerzuspiegeln.

Diese acht Muster wurden mithilfe eines eleganten maschinellen Lernverfahrens für das Clustering identifiziert und bilden komplexe Interaktionszusammenhänge sowie das Geschehen im Verlauf einer Sicherheitsverletzung besser ab. Dadurch eignen sie sich unter anderem als Grundlage für praktische Empfehlungen zur Prävention entsprechender Vorfälle.

Social Engineering

Psychologische Manipulation, die das Opfer zu einer Handlung verleiten soll, die grundlegende Datenschutzprinzipien verletzt

Menschliche Fehler leisten noch immer 82 % aller Sicherheitsverstöße Vorschub, und ein großer Teil dieser Vorfälle entfällt auf dieses Angriffsmuster. Hinzu kommt, dass Angreifer sich mit Social Engineering nicht nur Zugang zu einer Umgebung verschaffen, sondern oft auch Malware einschleusen oder Zugangsdaten stehlen, um dann in einem zweiten Schritt noch mehr Schaden anzurichten. Das unterstreicht, wie wichtig die Sensibilisierung der Mitarbeiter für diese Gefahr ist.

- Bei 59 % der untersuchten Social-Engineering-Angriffe wurden Anmeldedaten gestohlen und bei 31 % wurden gestohlene Anmeldedaten genutzt. Bei Social-Engineering-Angriffen ist die Wahrscheinlichkeit, dass Anmeldedaten gestohlen werden, dreimal höher als bei den anderen Angriffs- und Vorfallsmustern.
- Phishing wird bei diesen Angriffen doppelt so häufig genutzt wie das sogenannte Pretexting, bei dem der Angreifer einen Vorwand schafft, um Kontakt zu seinem Opfer herzustellen.
- Finanzielle Bereicherung tritt bei Social-Engineering-Angriffen achtmal häufiger als Motiv auf als Spionage.

Einfache Angriffe auf Web-Anwendungen

Vorfälle, bei denen die Angreifer eine Web-Anwendung kapern und danach nur wenige weitere Schritte oder zusätzliche Aktionen durchführen

In den meisten Fällen missbrauchen sie dabei gestohlene Anmeldedaten, um sich Zugang zu den über das Internet erreichbaren Infrastrukturkomponenten eines Unternehmens (wie Webserver oder E-Mail-Server) zu verschaffen.

- Bei vier von fünf Angriffen auf Web-Anwendungen werden gestohlene Anmeldedaten verwendet. Dieses Ergebnis unterstreicht die Bedeutung strenger Passwortrichtlinien.
- Einfache Angriffe auf Web-Anwendungen dienen mit viermal höherer Wahrscheinlichkeit Spionagezwecken als andere Angriffskategorien. Das lässt den Schluss zu, dass im staatlichen Auftrag handelnde Hacker bereitwillig auf komplexe Angriffe verzichten, wenn sie ihre Ziele mit einfacheren Methoden erreichen können.
- Im Kontext der einfachen Angriffe auf Web-Anwendungen ist der Missbrauch gestohlener Anmeldedaten sechsmal wahrscheinlicher als die Ausnutzung vorhandener Schwachstellen.

System Intrusion

Komplexe Angriffe, bei denen Malware und/oder Hackermethoden zur Einschleusung von Ransomware oder zur Realisierung anderer Zielsetzungen eingesetzt werden

Mit diesem Muster werden komplexe Angriffe beschrieben, die sich durch eine Kombination mehrerer Aktivitäten (wie Social Engineering, Malware und Hacking) auszeichnen. Angriffe über Lieferketten und Ransomware sind zwei Varianten dieses Musters, die in diesem Jahr stark gestiegen sind.

- 92 % der System Intrusions sind finanziell motiviert.
- Im Kontext von System Intrusions ist der Missbrauch gestohlener Anmeldedaten viermal wahrscheinlicher als die Ausnutzung vorhandener Schwachstellen.

Diverse Fehler

Vorfälle, bei denen die Sicherheit von Datenbeständen durch unbeabsichtigte Handlungen gefährdet wird Abhandengekommene Geräte gehören nicht zu dieser Kategorie, da sie bereits im Muster „Verlorene und gestohlene Ressourcen“ enthalten sind.

Die diesjährigen Daten zeigen, welch wichtige Rolle die Mitarbeiter spielen. Die beiden häufigsten Varianten „diverser Fehler“ sind Falschzustellungen und Fehlkonfigurationen. Fehlkonfigurationen werden häufig im Zusammenhang mit der Erkennungsmethode „Sicherheitsforscher“ genannt.

- Falsch konfigurierte Server, die infolge solcher Fehler über das Internet erreichbar sind, und der Versand von E-Mails an falsche Empfänger („Falschzustellungen“) machen 13 % aller Sicherheitsverstöße aus.
- Im Vorjahresvergleich sind externe Cloud-Speicher um 83 % seltener die Ursache für Sicherheitsverletzungen der Kategorie „diverse Fehler“. Das ist möglicherweise ein Hinweis auf die verstärkte Nutzung standardmäßig sicherer Technologien („Secure by Default“).
- 85 % der Sicherheitsverletzungen dieser Kategorie betreffen Server.

Missbrauch von Nutzerrechten

Sicherheitsvorfälle rund um die unbefugte oder böswillige Nutzung legitimer Zugriffsrechte

Die meisten Vorfälle dieser Art führen zu Datendiebstahl. Die Täter sind nach wie vor in der Regel finanziell motiviert und stehlen personenbezogene Daten, weil diese sich leicht zu Geld machen lassen.

- Im Vergleich zu allen anderen Kategorien sind von diesen Sicherheitsverletzungen mit dreimal höherer Wahrscheinlichkeit Dokumente betroffen.

Verlorene und gestohlene Ressourcen

Sicherheitsvorfälle, bei denen IT-Assets verloren gehen oder entwendet werden

Diebstahl ist in der Regel finanziell motiviert und wir gehen davon aus, dass auch IT-Ressourcen oft mit der Absicht gestohlen werden, sich am Weiterverkauf zu bereichern.

- Die von diesen Verbrechen betroffenen Daten sind (fast) haargenau dieselben wie im letzten Jahr. Während Diebstahl in der Regel von Außenstehenden begangen wird, sind für verlorene Assets natürlich Mitarbeiter verantwortlich.
- Die Täter gehören mit 14 Mal höherer Wahrscheinlichkeit keiner organisierten Gruppe an als bei anderen Vorfallsmustern.

Denial-of-Service

Angriffe auf Netzwerk- oder Anwendungsebene, die die Verfügbarkeit von Netzwerken und Systemen beeinträchtigen

Große Unternehmen werden doppelt so häufig mit Denial-of-Service-Attacken (DoS-Attacken) angegriffen wie mit den anderen Angriffs- und Vorfallsmustern. Für viele sind sie kaum mehr als ein Ärgernis, doch einige sind so häufig betroffen, dass es ihr Geschäftsmodell beeinträchtigt.

Alles Andere

Dies ist keine echte „Kategorie“, sondern ein Sammelbecken für alle Vorfälle, die sich keinem der anderen Muster zuordnen lassen.

Berg- und Tagebau, Öl und Gas sowie Versorgung

Dieser Sektor ist mit ähnlichen Bedrohungen wie die anderen von uns untersuchten Branchen konfrontiert, wie dem Diebstahl von Anmeldedaten und Ransomware. Außerdem sind jedoch auch Phishing und andere Social-Engineering-Angriffe weit verbreitet.

Muster im Zeitverlauf	Fünfjahres-trend	Dreijahres-trend	Vergleich mit anderen Branchen
Einfache Angriffe auf Web-Anwendungen	Unverändert	Unverändert	Rückläufig
Social Engineering	Unverändert	Unverändert	Unverändert
System Intrusion	Unverändert	Unverändert	Rückläufig

Berg- und Tagebau, Öl- und Gasindustrie plus Versorgungsbetriebe (oder BTÖGV, wie wir es liebevoll nennen) ist fast schon ein Zungenbrecher. In dieser interessanten „kombinierten“ Branche sind überdurchschnittlich viele Ingenieure tätig. Vielleicht zieht das die anderen – die Social Engineers – an. Jedenfalls liegt der Anteil der Social-Engineering-Angriffe über dem Durchschnitt der anderen Branchen.

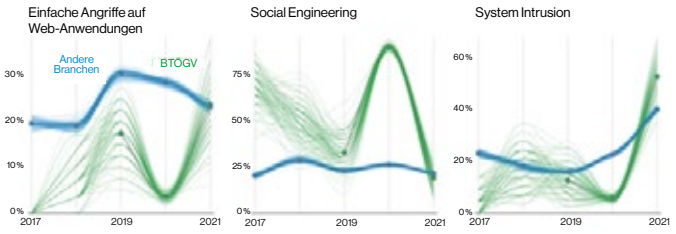

Abbildung 1: Häufigste Muster im BTÖGV-Sektor im Zeitverlauf

Absolute Häufigkeit	403 Vorfälle, davon 179 mit bestätigten Datenlecks
Top-Muster	Social Engineering, System Intrusions und einfache Angriffe auf Web-Anwendungen: 95 % der bestätigten Sicherheitsverletzungen
Urheber der Bedrohungen	Bestätigte Sicherheitsverletzungen: Externe Angreifer (96 %), Insider (4 %)
Motive der Angreifer	Bestätigte Sicherheitsverletzungen: Finanzielle Motive (78 %), Spionage (22 %)
Betroffene Daten	Bestätigte Sicherheitsverletzungen: Anmeldedaten (73 %), Personenbezogene Daten (22 %), Interna (9 %)
Empfohlene Abwehrmaß-nahmen (CIS Controls für IG1)	Schulungen zur Steigerung des Sicherheits-bewusstseins (CSC 14), Zugangskontrolle (CSC 6), Management von Nutzerkonten (CSC 5)
Anhaltende Trends	Die Branche wird nach wie vor sowohl von finanziell motivierten Kriminellen als auch von Industriespionen angegriffen.

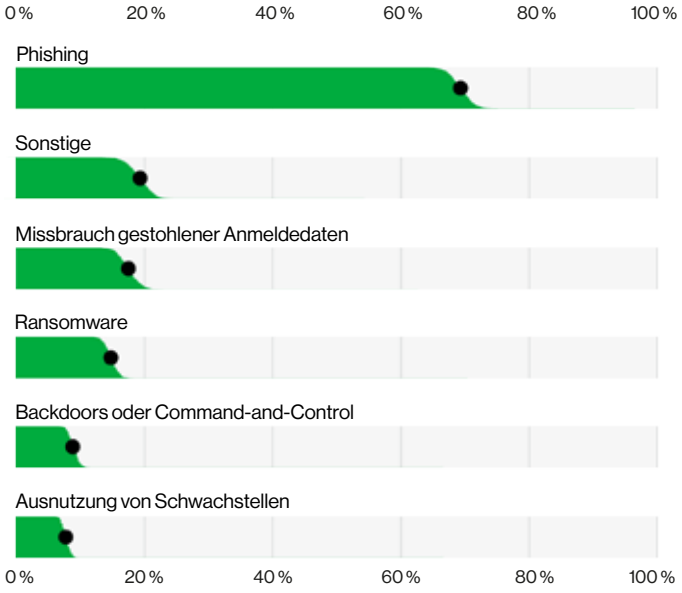

Abbildung 2: Häufigste Methoden bei Angriffen im BTÖGV-Sektor (n=153)

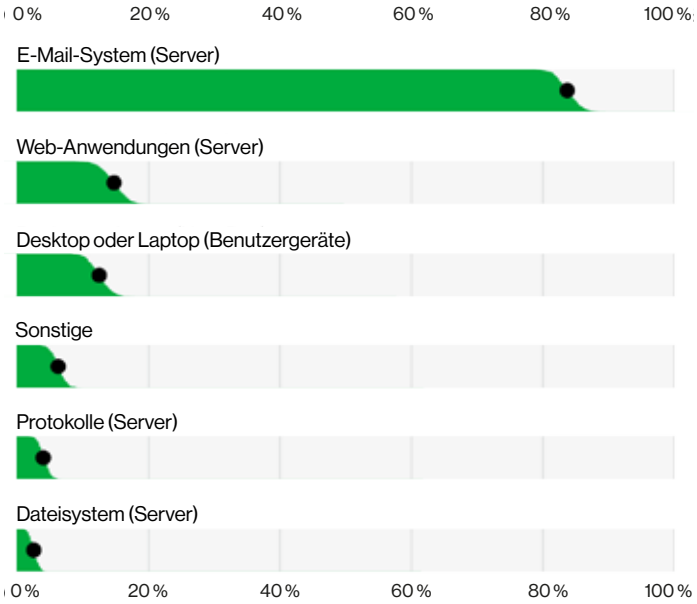

Abbildung 3: Am häufigsten betroffene Ressourcen bei Angriffen im BTÖGV-Sektor (n=130)

Vertrauen in unsere Daten

Seit dem DBIR 2019 weist die schräge rechte Kante der Balken in unseren Balkendiagrammen darauf hin, dass man in der Informationssicherheit nichts mit absoluter Gewissheit sagen kann.

Die Abschrägung zeigt das 95-%-Konfidenzintervall an (den Standardwert für statistische Tests).

Spaghetti-Diagramme und die relativ neuen Piktogramm-Plots sollen die inhärente Ungewissheit auf ähnliche Weise abbilden, sind aber besser für eine einzige Proportion geeignet.

Das spiegelt sich auch in der relativen Häufigkeit der Angreiferaktivitäten wider. Bei über 60 % handelt es sich um Phishing (siehe Abbildung 2), gefolgt vom Missbrauch gestohlener Anmeldedaten (die möglicherweise durch Phishing erbeutet wurden) und Ransomware (wobei Phishing ebenfalls eine Rolle spielen könnte). Angesichts der wichtigen Rolle dieser Branche für unser Wohlbefinden hoffen wir, dass kritische Infrastrukturen nicht nur durch Anmeldedaten geschützt werden, denn das ist einer der am häufigsten gestohlenen Datentypen.

Da Phishing und der Missbrauch von Anmeldedaten so weit verbreitet sind, überrascht es nicht, dass E-Mail-Server die am häufigsten angegriffenen Ressourcen in dieser Branche sind, gefolgt von Web-Anwendungen und Desktops. Obwohl die zum Betrieb dieser komplexen Systeme genutzten Infrastrukturen keine konventionellen IT-Infrastrukturen sind, können sie genau denselben Bedrohungen zum Opfer fallen wie die Infrastrukturen jedes anderen Unternehmens.

Halten Sie sich und Ihr Team auf dem Laufenden

Um den aktuellen Bedrohungen in den Branchen Berg- und Tagebau, Öl und Gas sowie Versorgungsunternehmen die Stirn bieten zu können, benötigen Sie zuverlässige Informationen. Deshalb bietet Ihnen die vollständige Ausgabe des DBIR einen detaillierten, praxisrelevanten Überblick über die Ziele, Methoden und Aktivitäten der Angreifer.

Den vollständigen DBIR 2022 finden Sie unter https://www.verizon.com/business/de-de/resources/reports/dbir/.