IBM **Security**

X-Force Threat Intelligence Index 2022: Zusammenfassung

IBM

Inhalt

Kurzer Überblick

Die Welt muss sich weiterhin mit einer anhaltenden Pandemie auseinandersetzen, mit Wechsel zwischen Homeoffice und Rückkehr ins Büro sowie mit geopolitischen Veränderungen, die einen beständigen Grundton von Misstrauen hervorbringen. All dies ist mit Chaos gleichzusetzen, und im Chaos gedeihen Cyberkriminelle. Im Jahr 2021 konnte IBM® Security XForce® beobachten, wie Bedrohungsakteure eine sich verändernde Landschaft opportunistisch nutzten, um Taktiken und Techniken zu übernehmen, mit denen sie Organisationen auf der ganzen Welt erfolgreich infiltrieren konnten.

Der IBM Security X-Force Threat Intelligence Index bildet neue Trends und Angriffsmuster ab, die wir anhand unserer Daten beobachtet und analysiert haben – diese stammen aus Milliarden von Datenpunkten, die von Erkennungsgeräten in Netzwerken und Endgeräten, aus der Behebung von Störfällen (IR), der Nachverfolgung von Domänennamen und anderem geliefert wurden. Dieser Bericht stellt die Ergebnisse dieser Recherche dar, welche auf Daten basiert, die von Januar bis Dezember 2021 erfasst wurden.

Wir bieten diese Erkenntnisse IBM Kunden, Forschern in der Sicherheitsbranche, Entscheiduntsträgern in der Politik, den Medien und der weiteren Community von Sicherheitsfachleuten und Führungskräften von Unternehmen als Ressource an.

Angesichts der unberechenbaren Umgebung und der Weiterentwicklung sowohl der Bedrohungstypen als auch der Träger der Bedrohung benötigen Sie Einblicke in Bedrohungsdaten, um Angreifern immer einen Schritt voraus zu sein und Ihre geschäftskritischen Assets mehr denn je zu stärken.

Report Highlights

Häufigster Angriffstyp: Ransomware war auch 2021 der häufigste Angriffstyp, obwohl sich der Prozentsatz der von X-Force behobenen Angriffe, bei denen es sich um Ransomware handelte, im Jahresvergleich um fast 9 % verringerte. REvil – ein Typ von Ransomware, der von X-Force auch als Sodinokibi bezeichnet wird, – war der verbreitetste Ransomware-Stamm, der von X-Force bereits das zweite Jahr beobachtet wurde, und machte 37 % aller Ransomware-Angriffe aus, gefolgt von Ryuk mit 13 %. Strafverfolgungsaktivitäten sind wahrscheinlich die primäre Kraft gewesen, Ransomware- und IoT-Botnet-Angriffe im Jahr 2021 zu reduzieren, aber dies schließt ein potenzielles Wiederaufleben im Jahr 2022 nicht aus.

Sicherheitslücken der Lieferketten: Die Aufmerksamkeit der Regierung und der politischen Entscheidungsträger wurde vorrangig auf die Sicherheit der Lieferketten gelenkt, auch durch den Ausführungserlass der Biden-Administration zur Cybersecurity und durch die Anweisung des US-Heimatschutzministeriums, der CISA und des NIST. Diese Richtlinien richten ein Spotlight auf Schwachstellen und Vertrauensbeziehungen. Das Ausnutzen von Schwachstellen war der wichtigste anfängliche Träger von Angriffen in der Fertigung, einer Branche, die mit den Auswirkungen von Druck und Verzögerungen in den Lieferketten zu kämpfen hat.

Die vom Phishing am meisten betroffenen Marken: X-Force hat im Laufe des Jahres 2021 genau verfolgt, wie Cyberkriminelle Phishing-Kits verwenden, und unsere Recherche ergab, dass Microsoft, Apple und Google die wichtigsten drei Marken waren, die Kriminelle zu imitieren versuchten. Diese Megamarken wurden wiederholt in Phishing-Kits verwendet, wobei Angreifer wahrscheinlich versuchten, Kapital aus deren Beliebtheit und dem Vertrauen zu schlagen, das viele Verbraucher in diese setzen.

Wichtigste Bedrohungsgruppen: Mutmaßlicher iranischer staatlicher Akteur, von dem eine Sicherheitsbedrohung ausgeht, ITG17 (MuddyWater), Cyberkriminelle Gruppe ITG23 (Trickbot) und Hive0109 (LemonDuck) waren einige der aktivsten Gruppen, die Analysten von X-Force Intelligence im Jahr 2021 beobachteten. Weltweit versuchten Bedrohungsgruppen, ihre Fähigkeiten zu erweitern und mehr Organisationen zu infiltrieren. Die von ihnen verwendete Schadsoftware war in größere Techniken zum Umgehen der Verteidigung eingebettet, in manchen Fällen über cloudbasierte Messaging- und Speicherplattformen gehostet, um die Sicherheitskontrollen zu überwinden. Diese Plattformen wurden missbraucht, um Befehls- und Kontrollkommunikation im legitimen Netzverkehr zu verbergen. Bedrohungsakteure entwickelten auch weiterhin Linux-Versionen von Schadsoftware, um damit leichter in Cloud-Umgebungen gelangen zu können.

Wichtige Statistiken

21 %

Ransomware-Anteil von Angriffen
Ransomware war der von X-Force beobachtete Angriffstyp Nummer eins im letzten Jahr, wobei die Anzahl der Angriffe von 23 % im Vorjahr auf 21 % gesunken ist. REvil Ransomware-Akteure (alias Sodinokibi) waren für 37 % aller Ransomware-Angriffe verantwortlich.

17 Monate

Durchschnittliche Zeit bevor eine Ransomware-Gruppe ihren Namen ändert oder inaktiv wird
Von X-Force untersuchte Ransomware-Gruppen hatten eine mittlere Lebensdauer von 17 Monaten bis zum Wechsel ihres Namens oder zu ihrer Auflösung. REvil, eine der erfolgreichsten Gruppen, löste sich im Oktober 2021 nach 31 Monaten (zweieinhalb Jahren) auf.

41 %

Prozentsatz der Angriffe, die Phishing für den Erstzugriff ausnutzen
Phishing-Aktivitäten haben sich 2021 als wichtigster Weg zur Kompromittierung herausgestellt, wobei 41 % der von X-Force behobenen Vorfälle sich dieser Technik bedienten, um einen Erstzugriff zu gewinnen.

33 %

Anstieg der Zahl der Vorfälle von 2020 auf 2021 durch Ausnutzen von neuen Schwachstellen
Vier der fünf wichtigsten im Jahr 2021 ausgenutzten Schwachstellen waren neue Schwachstellen, darunter die Log4j- Schwachstelle CVE-2021-44228, – die auf Platz zwei landete, obwohl sie erst im Dezember bekannt wurde.

3X

Klick-Wirksamkeit bei gezielten Phishing-Kampagnen, die zusätzlich Telefonanrufe nutzen
Die Klickrate für die durchschnittliche gezielte Phishing-Kampagne lag bei 17,8 %, aber gezielte Phishing-Kampagnen, die zusätzlich Telefonanrufe nutzten (Vishing oder Telefon-Phishing), waren dreimal so effektiv, da sie von 53,2 % der Opfer einen Klick einfingen.

146 %

Zunahme von Linux-Ransomware mit neuem Code

Der Prozentsatz von Linux-Ransomware mit eindeutigem (neuem) Code stieg nach Angaben von Intezer im Jahresvergleich um 146 %, was auf einen Anstieg des Innovationsniveaus der Linux-Ransomware hindeutet.

Nr. 1

Angriffsziel ist die Fertigungsbranche

Die Fertigungsbranche ersetzte 2021 die Finanzdienstleister als hauptsächliches Angriffsziel, was 23,2 % der Angriffe entspricht, die X-Force im letzten Jahr behoben hat. Ransomware war der häufigste Angriffstyp und machte 23 % der Angriffe auf Fertigungsunternehmen aus.

61 %

Fertigungsanteil an Gefährdungen von Organisationen in Zusammenhang mit OT

Einundsechzig Prozent der Vorfälle bei mit OT verbundenen Organisationen im letzten Jahr ereigneten sich in der Fertigungsbranche. Hinzu kommt, dass 36 % der Angriffe auf OT nutzende Organisationen Ransomware Attacken waren.

2.204 %

Zunahme der Ausspähung gegen OT

Angreifer steigerten ihre Ausspähung von SCADA Modbus OT-Geräten, die über das Internet zugänglich waren, zwischen Januar und September 2021 um 2.204 %.

74 %

Anteil der IoT-Angriffe, die vom Mozi Botnet ausgingen

Im Jahr 2021 gingen Angriffe auf IoT-Geräte in 74 % der Fälle vom Mozi- Botnet aus.

26 %

Anteil weltweiter Angriffe, die auf Asien abzielten

Sechsundzwanzig Prozent aller Angriffe hatten Ziele in Asien im Fadenkreuz.
Asien war die am stärksten angegriffene geografische Region des Jahres 2021.

Empfehlungen zur Risikominderung

Die Bedrohungen, die wir in diesem Bericht vorgestellt haben, haben das Potenzial, zu Sorge Anlass zu geben, da der Bericht das schwere und zunehmende Sicherheitsrisiko durch Ransomware und erneute Bedrohungen durch BEC und Phishing unterstreicht und mehrere Zero-Day-Exploits hervorhebt, die bedrohende Akteure im vergangenen Jahr ausgenutzt haben. Unsere Absicht ist es jedoch, mit diesen Informationen Organisationen zu ermächtigen, die aktuelle Bedrohungsumgebung besser zu verstehen, und Hilfe beim Aufbau von Zuverlässigkeit bei den Aktionen zu leisten, die sie ergreifen müssen, um diese Bedrohungen zu bekämpfen.

Einige Sicherheitsprinzipien, die X-Force als hilfreich bei der Bekämpfung heutiger Cyber-Bedrohungen befunden hat, sind unter anderem ein Zero-Trust-Ansatz, Automatisierung der Reaktion auf Vorfälle und erweiterte Erkennungs- und Reaktionsfähigkeiten.

Ein Zero-Trust-Ansatz hilft, das Risiko von gewichtigen Angriffen zu verringern

Der Zero-Trust-Ansatz ist ein Paradigmenwechsel, eine neue Herangehensweise an Sicherheitsprobleme, die davon ausgeht, dass eine Verletzung bereits stattgefunden hat, und zielt darauf ab die Schwierigkeit für einen Angreifer zu erhöhen, sich durch ein Netzwerk zu bewegen. Im Kern geht es darum zu verstehen, wo sich kritische Daten befinden und wer Zugriff auf diese Daten hat, und um stabile Überprüfungsmaßnahmen im gesamten Netzwerk zu erstellen, um sicherzustellen, dass nur berechtigte Personen auf diese Daten in der richtigen Weise zugreifen.

Untersuchungen der Bedrohungsforscher von X-Force bestätigen, dass Grundsätze verbunden mit einem Zero-Trust-Konzept – einschließlich der Implementierung von MFA und dem Prinzip des geringsten Privilegs – das Potenzial haben, die Anfälligkeit von Organisationen gegenüber den in diesem Bericht identifizierten wesentlichen Angriffsarten insbesondere Ransomware und BEC zu verringern.

Die Anwendung des Prinzips des geringsten Privilegs auf Domänencontroller und insbesondere Konten von Domänenadministratoren kann Barrieren für Ransomware-Akteure erhöhen, da viele dieser Akteure versuchen, Ransomware auf einem Netzwerk von einem beeinträchtigten Domänencontroller bereitzustellen. Zusätzlich erhöht die Implementierung von MFA die Schwierigkeit für Cyberkriminelle, die versuchen, E-Mail-Konten zu übernehmen, indem sie verlangen, dass über gestohlene Berechtigungsnachweise hinaus weitere Authentifizierung zur Verfügung gestellt werden.

Erfahren Sie mehr darüber, wie Sie einen Zero-Trust-Ansatz aufbauen können →

Sicherheitsautomatisierung verbessert die Behebung von Störfällen

Das X-Force Incident Response Team befasst sich jedes Jahr mit Hunderten von Vorfällen in verschiedensten Geografien und unterstützt unternehmensintern Analysten bei der Behebung von Störfällen und der Behandlung von einer Vielzahl an Angriffsarten. Geschwindigkeit ist von entscheidender Bedeutung, sei es das Identifizieren und Ausschalten von bedrohenden Akteuren bevor sie Ransomware in einem Netzwerk einsetzen können, oder die schnelle und effiziente Behebung von Problemen, um Kapazität für den nächsten Vorfall zu schaffen. In dieser schnelllebigen Umgebung ist die Automatisierung der Sicherheit wichtig – die Auslagerung von Aufgaben an Maschinen, für die ein menschlicher Analyst oder ein Team Stunden brauchen könnte, und die Identifizierung von Mechanismen zur Verbesserung der Arbeitsabläufe.

Mitte 2021 spendete IBM der Open Cybersecurity Alliance ein Automatisierungstool zum Aufspürgen von Bedrohungen, das darauf abzielt, Analysten des Security Operations Center (SOC) dabei zu unterstützen, forensische Untersuchungen schnell durchzuführen und Cyber-Vorfälle rasch zu beheben. Darüber hinaus setzt das X-Force IR Team IBM Security QRadar SOAR ein, um seine Reaktionsfähigkeiten auf Vorfälle zu verbessern.

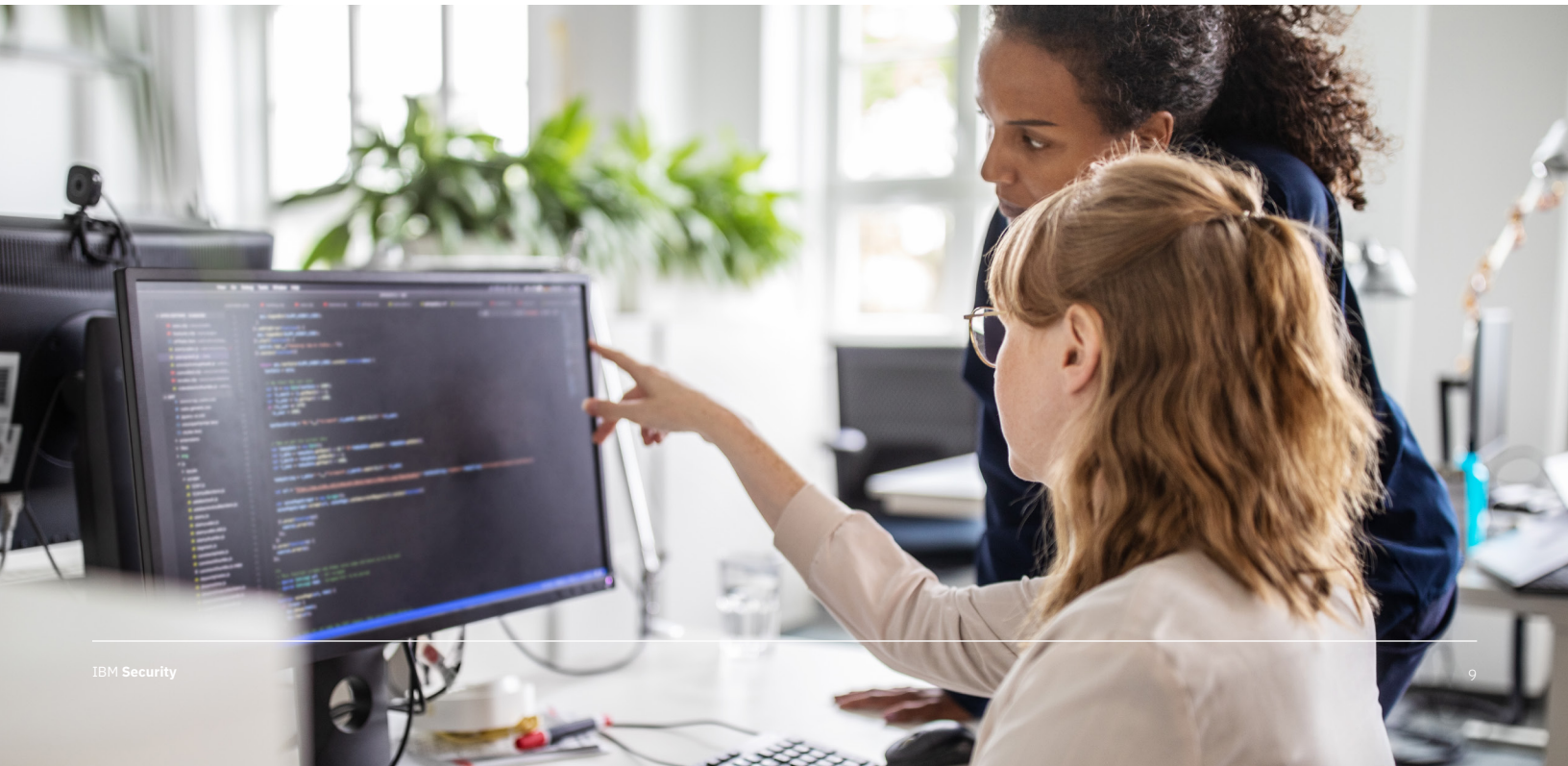
Erfahren Sie mehr über die Services von IBM zur Behebung von Störfällen →

Erweiterte Erkennung und Reaktion bieten einen erheblichen Vorteil gegenüber Angreifern

Technologien zur Erkennung und Intervention – insbesondere wenn mehrere unterschiedliche Lösungen zu einer erweiterten Erkennungs- und Interventionslösung (XDR) kombiniert werden – bieten Organisationen einen erheblichen Vorteil, wenn es darum geht, Angreifer zu identifizieren und aus einem Netz zu entfernen, bevor sie das Ziel ihres Angriffs erreichen können, wie etwa den Einsatz von Ransomware oder Datendiebstahl.

In mehreren Fällen, in denen das X-Force IR-Team eine Endpunkterkennung (EDR) oder eine XDR- Lösung im Netzwerk eines Kunden implementierte, hat IR sofort zusätzliche Erkenntnisse gewonnen, die bei der Identifizierung der Aktivitäten von Angreifern und bei deren rascher Behebung geholfen haben. XDR-Technologien helfen wahrscheinlich, die Zunahme von Serverzugriff und anderen Angriffsarten voranzutreiben, die X-Force beobachtet und die anzeigen, dass ein Angreifer identifiziert und gestoppt wurde, bevor der Vorgang sein beabsichtigtes Ende erreichen konnte.

Erfahren Sie mehr über IBM Security QRadar XDR →



Empfehlungen

Die folgenden Empfehlungen schließen bestimmte Maßnahmen ein, die Organisationen ergreifen können, um ihre Netzwerke besser vor den in diesem Bericht vorgestellten Bedrohungen zu schützen.

Entwickeln Sie einen Reaktionsplan gegen Ransomware. Jede Branche und jede geografische Region ist dem Risiko eines Ransomware-Angriffs ausgesetzt, und wie Ihr Team zum kritischen Zeitpunkt reagiert, kann den Unterschied dabei ausmachen, wie viel Zeit und Geld bei einer Reaktion verloren geht.

— Nehmen Sie in Ihren Reaktionsplan sofortige Eindämmungsmaßnahmen auf, welche Interessengruppen und Strafverfolgungsbeamte informiert werden sollten, wie Ihre Organisation Sicherheitskopien anlegen und von diesen zurückspeichern wird und eine alternative Speicherposition, von der aus wichtige Geschäftsfunktionen während der Behebung ausgeführt werden können.

— Beziehen Sie in Ihren Plan ein Szenario von Datendiebstahl und Datenleck als Teil des Ransomware-Angriffs mit ein – dies ist eine sehr gängige Taktik, die heute verwendet wird und bei einem sehr hohen Prozentsatz von Ransomware-Angriffen zu sehen ist, die X-Force behebt.

— Nutzen Sie Ransomware-Drills, um auch zu überlegen, ob Ihre Organisation ein Lösegeld zahlen würde, und welche Faktoren Ihre Berechnung für diese Entscheidung ändern würden.

— Stellen Sie sicher, dass Ihr Ransomware-Reaktionsplan einen speziellen Notfallplan für einen Cloud-bezogenen Vorfall enthält, da dieser möglicherweise zusätzliche Tools und Fähigkeiten erfordert.

— Vermeiden Sie Datenverlust durch Schadsoftware oder Ransomware-Angriffe mit Flashspeicherlösungen, die Datenverlust verhindern, einen durchgängigen Betrieb fördern und niedrigere Infrastrukturkosten mit sich bringen.

— Der Definitive Leitfaden zu Ransomware von X-Force gibt zusätzliche detaillierte Ratschläge, wie Sie auf einen Ransomware-Angriff reagieren sollten. Das X-Force Incident-Response Team kann auch eine Bewertung der Ransomware-Bereitschaft für Ihre Organisation durchführen, um Ihnen beim Aufbau und Test eines Ransomware- Vorfallplans zu helfen. Das X-Force Command-Center bereitet Unternehmen auf ähnliche Weise auf einen Ransomware-Angriff vor, wobei sowohl die organisatorische als auch die erforderliche technische Intervention berücksichtigt wird.

Mehrfaktorauthentifizierung an jedem Remotezugriffspunkt auf ein Netzwerk implementieren. X-Force hat beobachtet, dass mehr Unternehmen MFA erfolgreicher als je zuvor implementieren. Dies verändert die Bedrohungslandschaft buchstäblich, da bedrohende Akteure gezwungen sind, neue Wege zur Kompromittierung von Netzwerken zu finden, statt gestohlene Zugangsdaten auszunutzen, wodurch die Wirksamkeit von E-Mail-Übernahmekampagnen verringert wird.

— MFA kann das Risiko mehrerer verschiedener Angriffstypen verringern, darunter Ransomware, Datendiebstahl, BEC und Serverzugriff.

— Außerdem machen Technologien für Identitäts- und Zugriffsmanagement die MFA-Implementierung jedes Jahr einfacher, – sowohl für Implementierungsteams als auch für Endbenutzer.

Ergreifen Sie einen mehrschichtigen Lösungsansatz zur Bekämpfung von Phishing. Leider gibt es heute kein einziges Tool oder Lösung, die alle Phishing-Angriffe verhindern kann, und die Bedrohungsakteure verfeinern immer wieder ihre Social-Engineering- und Anti-Malware-Erkennungstechniken, um etablierte Kontrollen zu umgehen. Daher empfehlen wir die Implementierung mehrschichtiger Lösungen, die eine höhere Wahrscheinlichkeit haben, Phishing-E-Mails abzufangen.

— Erstens sind ein wirksames Benutzerbewusstsein und effiziente Ausbildung wichtig und sollten realistische Beispiele einschließen.

— Zweitens sollten Sie eine E-Mail-Softwaresicherheitslösung einsetzen, um eine Maschine mit der Aufgabe der Identifizierung und des Ausfilterns von schädlichen Nachrichten zu befassen.

— Drittens sollten Sie mehrere Abwehrmechanismen implementieren, die Schadsoftware oder eine Lateralausbreitung rasch abfangen können, falls eine Phishing-E-Mail durchrutschen sollte, einschließlich einer verhaltensbasierten Erkennung von Schadsoftware, Endpoint Detection and Response (EDR), Intrusion Detection und Präventionslösungen (IDPS) und eines Systems für Security-Information und Event-Management (SIEM).

Verfeinern Sie Ihr Schwachstellenmanagementsystem und bauen Sie es aus. Schwachstellenmanagement ist eine Kunst – von der Identifizierung, welche Schwachstellen für die Netzarchitektur Ihres Unternehmens am zutreffendsten sind, bis hin zur Identifizierung von Vorgehensweisen diese zu schließen, ohne laufende Prozesse zu beeinträchtigen.

— Ein eigenes Team für das Schwachstellenmanagement zu haben und sicherzustellen, dass dieses Team gut ausgestattet ist und unterstützt wird, kann den entscheidenden Unterschied ausmachen, um sicherzustellen, dass Ihr Netzwerk vor der Ausnutzung von potenziellen Schwachstellen geschützt ist.

— Wir empfehlen die Priorisierung aller in dieser Beurteilung erwähnten Schwachstellen, die auf Ihre Organisation zutreffen.

— IBMs X-Force Exchange enthält auch ein Repository mit Schwachstellen und zugeordneten Gefährlichkeitsstufen, um Sie bei der Identifizierung der bedenklichsten Schwachstellen zu unterstützen, und X-Force Red kann spezialisierte Services zum Ermitteln und für das Management von Sicherheitslücken zur Verfügung stellen.

Weitere Informationen erhalten Sie im Gesamtbericht →

Informationen zu IBM Security X-Force

IBM Security X-Force ist ein auf Bedrohungen ausgerichtetes Team aus Hackern, Respondern, Forschern und Analysten. Unser Portfolio umfasst offensive und defensive Produkte und Services, die durch eine 360-Grad-Sicht auf Bedrohungen angetrieben sind. Mit X-Force als Ihrem Sicherheitspartner können Sie verlässlich behaupten, dass die Wahrscheinlichkeit und die Auswirkung einer Datenschutzverletzung minimal sind.

IBM Security X-Force Threat Intelligence kombiniert IBM Security Operations Telemetrie, Forschung, Incident-Response-Untersuchungen, kommerzielle Daten und offene Quellen, um Kunden dabei zu unterstützen, aufkommende Bedrohungen zu verstehen und schnell fundierte Sicherheitsentscheidungen zu treffen.

Zusätzlich bietet das X-Force Incident-Response Team Dienstleistungen zur Erkennung, Intervention, Behebung und Vorbereitung, um Ihnen zu helfen, die Auswirkung einer Datenschutzverletzung zu minimieren.

X-Force kombiniert mit den Erfahrungen des IBM Security Command Center schult Ihr Team – von Analysten bis hin zur Unternehmensleitung – damit es für die Realitäten heutiger Bedrohungen bereit ist. X-Force Red, das Hacker-Team von IBM Security, bietet offensive Sicherheitsservices, darunter Tests auf unbefugten Zugriff, Schwachstellenmanagement und Angriffssimulation.

Das ganze Jahr über stellen die IBM X-Force-Spezialisten außerdem fortlaufende Untersuchungen und Analysen in Form von Blogs, Whitepapers, Webinaren und Podcasts zur Verfügung, in denen sie die IBM-Erkenntnisse über raffiniert arbeitende Bedrohungsakteure, neue Malware und neue Angriffsmethoden vorstellen. Darüber hinaus bieten wir unseren Abonnement-Kunden über unsere Lösungen von X-Force Threat Intelligence einen umfangreichen Bestand an aktuellen, hochmodernen Analysen.

Vereinbaren Sie ein Gespräch mit einem unserer X-Force-Experten →

Informationen zu IBM Security

IBM Security arbeitet mit Ihnen zusammen, um Ihr Unternehmen mit einem fortschrittlichen und integrierten Portfolio an Sicherheitsprodukten und -services für Unternehmen zu schützen, die mit KI kombiniert sind und einen modernen Ansatz für Ihre Sicherheitsstrategie mit Zero-Trust-Prinzipien verfolgen. Durch die Anpassung Ihrer Sicherheitsstrategie an Ihr Unternehmen, die Integration von Lösungen zum Schutz Ihrer digitalen Anwender, Assets und Daten und die Bereitstellung von Technologien zur Verwaltung Ihrer Abwehrmaßnahmen gegen wachsende Bedrohungen assistieren wir Ihnen bei der Bewältigung und Handhabung von Risiken. Unsere Lösungen unterstützen die hybriden Cloud-Umgebungen von heute.

Unser neuer moderner, offener Ansatz, die IBM Cloud Pak for Security-Plattform, basiert auf RedHat Open Shift und unterstützt die heutigen hybriden Multi-Cloud-Umgebungen mit einem umfangreichen Partner-Ökosystem. Cloud Pak for Security ist eine unternehmenstaugliche, containerisierte Softwarelösung, die Ihnen ermöglicht, die Sicherheit Ihrer Daten und Anwendungen durch die schnelle Integration Ihrer bestehenden Sicherheitstools zu verwalten, um tiefere Einblicke in Bedrohungen in sämtlichen hybriden Cloud-Umgebungen zu generieren. Sie belässt Ihre Daten dort, wo sie sind, was eine einfache Orchestrierung und Automatisierung Ihrer Sicherheitsmaßnahmen ermöglicht.

Für weitere Informationen ziehen Sie bitte www.ibm.com/security heran oder besuchen Sie den IBM Security Intelligence Blog.

Mitwirkende

Camille Singleton
Charles DeBeck
Joshua Chung
David McMillen
Scott Craig
Scott Moore
Charlotte Hammond
John Dwyer
Melissa Frydrych
Ole Villadsen
Richard Emerson
Guy-Vincent Jourdan
Vio Onut
Stephanie Carruthers
Adam Laurie
Michelle Alvarez
Salina Wuttke
Georgia Prassinos
John Zorabedian
Mitch Mayne
Limor Kessem
Ian Gallagher
Ari Eitan

IBM Deutschland GmbH
IBM-Allee 1 71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95 1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106 8010 Zürich ibm.com/ch

Produziert in den USA Februar 2022