MANDIANT
NOW PART OF Google Cloud

Sonderbericht M-Trends 2023

Kurzfassung

M-Trends 2023, die 14. Ausgabe unseres Berichts, finden Sie jetzt unter www.mandiant.de/m-trends.

In Zahlen – die Datenquellen für M-Trends

Die Informationen stammen aus Untersuchungen, die Mandiant Consulting zwischen dem 1. Januar 2022 und dem 31. Dezember 2022 durchgeführt hat.

Wichtigste Punkte

- Weltweit werden Angriffe im Durchschnitt schneller erkannt. Das ist auf Verbesserungen in Nord- und Südamerika sowie der EMEA-Region (jedoch nicht in der APAC-Region) zurückzuführen.
- In den meisten Fällen informierten Sicherheitsanbieter und andere externe Quellen die betroffenen Unternehmen über einen Angriff, doch wenn interne Teams Sicherheitsverletzungen aufdeckten, waren sie in der Regel schneller als externe Quellen.
- Angreifer gehen in den einzelnen Regionen unterschiedlich vor: In Nord- und Südamerika nutzen sie vor allem Exploits, in der EMEA-Region Phishing-Kampagnen und in der APAC-Region Vorarbeit aus vorherigen Angriffen aus.

Fragen an Ihren CISO

- Wie messen wir die Zeit, die wir für die Bedrohungserkennung und -abwehr benötigen? Was ist unser Medianwert für die Zeit von der Bedrohungserkennung bis zur Abwehr und Fehlerbehebung?
- Sind wir auf die Erkennung der gängigsten Malwarevarianten, Exploits und Einschleusungsmethoden (wie Phishing) vorbereitet?
- Welchen Plan haben wir für den Fall, dass wir von Dritten über einen potenziellen Angriff informiert werden?
- Können wir Exploits von Systemen mit bekannten Sicherheitslücken verhindern?

Invasion der Ukraine

Wichtigste Punkte

- Mandiant hat nicht erst seit der russischen Invasion der Ukraine am 24. Februar 2022, sondern auch schon im Vorfeld weitreichende Cyberspionageaktivitäten, disruptive und destruktive Cyberangriffe und militärische Informationsoperationen aufgedeckt.
- Zu den russischen Zielen zählten industrielle Steuersysteme und kritische Infrastrukturen. Einige dieser Angriffe waren schon vor der Invasion mithilfe verschiedener Kampagnen vorbereitet worden.
- Der russische Angriffskrieg auf die Ukraine hat gezeigt, dass die Kombination aus Cyberoperationen und konventioneller (kinetischer) Kriegsführung bereits aktiv genutzt wird.

Fragen an Ihren CISO

- Haben wir unsere Systeme gehärtet, um sie vor destruktiven und disruptiven Angriffen zu schützen?
- Wie sind die letzten Tests unserer Back-up- und Geschäftskontinuitätsprozesse ausgefallen?
- Sollten wir Bedrohungsdaten nutzen, um militärische Informationsoperationen besser abwehren zu können?

Finanziell motivierte Angriffe aus Nordkorea

Wichtigste Punkte

- Neben den üblichen Cyberspionagekampagnen und disruptiven Angriffen haben sich Cyberkriminelle aus der Demokratischen Volksrepublik Korea im Jahr 2022 vor allem auf den Diebstahl – und die Nutzung – von Kryptowährungen verlegt.
- Da sich diese Kampagnen als äußerst lukrativ erwiesen haben, ist auch 2023 mit weiteren Angriffen zu rechnen.

Fragen an Ihren CISO

- Wie gut sind wir auf finanziell motivierte Angreifer vorbereitet, die auf unser Unternehmen abzielen könnten?

Neue Motive und ungewöhnliche Techniken

Wichtigste Punkte

- Auch technisch weniger versierte Angreifer richten großen Schaden in Unternehmen an.
- Dazu gehören Datendiebstahl, Diebstahl geistigen Eigentums und erhebliche Ruf- und Imageschäden.
- Diese Angreifer sind äußerst raffiniert und schrecken auch vor Bestechung oder aggressiven Drohungen nicht zurück, um ihre Ziele zu erreichen. Dabei scheint es ihnen weniger um Geld oder Daten zu gehen, sondern mehr darum, sich unter ihresgleichen einen Namen zu machen.

Fragen an Ihren CISO

- Wie minimieren wir die Risiken von Social-Engineering-Angriffen und ähnlichen Bedrohungen? Wie können wir verhindern, dass sie unsere Mitarbeiter erreichen?
- Wie schützen wir unsere Mitarbeiter, insbesondere Führungskräfte und Beschäftigte mit einem öffentlichen Profil, vor solchen Angriffen?
- Wie sollten wir reagieren, falls proprietäre Informationen oder personenbezogene Kundendaten gestohlen und als Druckmittel bei der Lösegeldforderung eingesetzt werden?
- Verfügen wir über einen Prozess, um im Fall einer Erpressung möglichst schnell Kryptowährung zu erwerben?

Cloud-Angriffe – eine Red-Team-Fallstudie

Wichtigste Punkte

- Bei Red-Team-Einsätzen werden die Sicherheitsprogramme von Unternehmen mit Angriffstechniken aus der Praxis getestet und Tipps zur Verbesserung des Sicherheitsniveaus gegeben.
- Die Experten von Mandiant demonstrierten einem Versorgungsunternehmen bei einem solchen Einsatz, wie Angreifer sich Zugriff auf kritische Ressourcen in Cloud- und OT-Umgebungen verschaffen könnten.

Fragen an Ihren CISO

- Haben wir einen umfassenden Überblick über die Cloud-Nutzung in unserem Unternehmen?
- Suchen wir regelmäßig nach Fehlkonfigurationen, die Angreifer ausnutzen könnten?
- Testen wir unsere Cloud-Architekturen?

Kampagnen und globale Ereignisse

Wichtigste Punkte

- Mandiant hat 2022 das Campaigns and Global Events-Team gegründet, das die russischen Spionageaktivitäten, Ransomware-Angriffe und schwerwiegende Sicherheitslücken wie Log4Shell genauer untersucht.
- Das Team informiert über wichtige Erkenntnisse und Indikatoren, damit unsere Kunden und die Allgemeinheit sich besser vor solchen Kampagnen und globalen Ereignissen schützen können.

Fragen an Ihren CISO

- Wie erfassen und patchen wir Sicherheitslücken in unserem Netzwerk?
- Wie nutzen wir aktuelle Bedrohungsdaten bei der Entscheidungsfindung?

APT42 – eine neu benannte Hackergruppe

Wichtigste Punkte

- APT42 ist eine Hackergruppe, die vermutlich von Iran gesponsert wird und Spionageangriffe mithilfe von komplexen Phishing- und Social-Engineering-Kampagnen durchführt.
- Die Aktivitäten von APT42 stellen eine Bedrohung für außenpolitische Beamte, Kommentatoren und Journalisten dar, insbesondere für diejenigen in den USA, im Vereinigten Königreich und in Israel, die an Projekten mit Bezug zum Iran arbeiten.

Fragen an Ihren CISO

- Mit welchen Maßnahmen können unsere Sicherheits-, IT- und Business-Teams alle Mitarbeiter noch besser schützen?
- Wie minimieren wir das Risiko, dass Mitarbeiter auf Social-Engineering-Kampagnen hereinfallen?
- Wie können wir unsere Mitarbeiter vor Phishing- und sonstigen Social-Engineering-Versuchen warnen?

Weitere Informationen finden Sie unter www.mandiant.de/m-trends.

Mandiant

11951 Freedom Dr, 6th Fl, Reston, Virginia 20190, USA Tel.: +1 703 935 1700
+1 833 3MANDIANT (362 6342)
info@mandiant.com

Über Mandiant

Mandiant ist als führender Anbieter von dynamischen Cyberabwehrlösungen, Threat Intelligence und Incident-Response-Services bekannt. Mandiant nutzt seine jahrzehntelange Praxiserfahrung, um Unternehmen und Institutionen bei der souveränen Prävention und Abwehr von Cyberbedrohungen zu unterstützen. Mandiant gehört nun zu Google Cloud.

MANDIANT
NOW PART OF Google Cloud