THREATQUOTIENT™

ThreatQ™ für Einzelhandel und Gastgewerbe

Cybersicherheitsverletzungen im Einzelhandel und Gastgewerbe sind vielleicht am schwerwiegendsten und nehmen in alarmierendem Maße zu. Laut einem Bericht von Thales wurden fast 75 Prozent der US-amerikanischen Einzelhändler schon einmal Opfer eines Angriffs, während es im Vorjahr noch 52 Prozent waren.[1] Einzelhändler und Unternehmen im Bereich Gastgewerbe investieren stark in Cybersicherheit, um Zahlungskartendaten sowie andere personenbezogene Daten zu schützen. Einzelhändler können ihre Marken jedoch besonders effektiv aus negativen Schlagzeilen heraushalten, wenn sie das folgende Sprichwort beachten: „Wer nicht aus der Vergangenheit lernt, ist dazu verdammt, sie zu wiederholen." Mit anderen Worten: Cyberkriminelle verwenden immer wieder die gleichen Taktiken, Techniken und Prozeduren (TTPs) und hinterlassen dabei sichtbare Spuren oder Indikatoren, die Einblicke in Bedrohungen liefern.

Es reicht jedoch nicht aus, Bedrohungsdaten-Feeds zu abonnieren. Vielmehr benötigen Unternehmen eine Möglichkeit, alle externen und internen Bedrohungsdaten zu aggregieren und zu deduplizieren. Anschließend müssen nicht relevante Daten herausgefiltert sowie relevante Informationen bewertet und priorisiert werden, um geeignete Gegenmaßnahmen zu ergreifen. Dadurch lässt sich die Zeit von der Erkennung bis zur Behebung verkürzen. Je schneller Teams diese Informationen importieren, ergänzen, bereitstellen und nutzen können, desto mehr Druck üben Verteidiger auf Angreifer aus, wodurch diese offensive und Flüchtigkeitsfehler machen. Durch die Nutzung von Bedrohungsinformationen können Teams von Branchenkollegen und deren Erfahrungen lernen, gegnerische TTPs erkunden und die eigenen Abwehrmaßnahmen proaktiv analysieren sowie verstärken, damit künftige Angriffe zuverlässig abgewehrt werden.

Laut einem 2018 von Thales veröffentlichen Bericht wurden 75 Prozent der US-amerikanischen Einzelhändler schon einmal Opfer eines Angriffs, während es im Vorjahr noch 52 Prozent waren.[2]

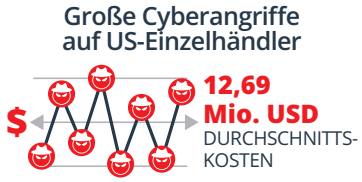
Einzelhändler sind dreimal häufiger von Angriffen betroffen als der Finanzsektor.[3]

WICHTIGE HERAUSFORDERUNGEN

PERSONENBEZOGENE DATEN UND ZAHLUNGSINFORMATIONEN

Personenbezogene Daten und Kreditkartendaten sind die Lebensader des Einzelhandels. Bei jeder Transaktion werden wertvolle Daten ausgetauscht, deren enorme Menge Einzelhändler zu lukrativen Zielen für Bedrohungsakteure macht. Sichere Zahlungstechnologien helfen zwar bei der Verstärkung der Abwehrmaßnahmen, sind aber keine Wunderwaffe. Wenn es *dennoch* zu erfolgreichen Angriffen kommt, führen diese einer Untersuchung von Visa zufolge zu noch schwerwiegenderen Sicherheitsverletzungen. Hervorzuheben ist außerdem, dass die Chip-Technologie von Europay, Mastercard und Visa (EMV) zwar die Sicherheit bei Transaktionen erhöht, die über Kassenterminals (POS) erfolgen, jedoch nichts zum Schutz von E-Commerce-Transaktionen beiträgt, bei denen keine Karte vorgezeigt werden muss.

SPEARPHISHING



Die Durchschnittskosten eines Cyberangriffs werden je großem US-Einzelhandelsunternehmen auf 12,69 Millionen US-Dollar geschätzt.[4]

Viele der gefährlichsten Angriffe Bedrohungen für den Einzelhandel und das Gastgewerbe nutzen Spearphishing-E-Mails, die sich fast gar nicht von legitimen E-Mails unterscheiden. Einige Kampagnen setzen auf einen schnellen, großflächigen Angriff, um mehrere Händler gleichzeitig und nach dem Schrotflintenprinzip anzugreifen. Andere wiederum nehmen den POS-Anbieter oder -Integrator des Händlers ins Visier, um sich Systemzugang zu verschaffen. Sobald die Angreifer den Weg ins Netzwerk gefunden haben, nutzen sie Schwachstellen aus, um Anmeldedaten zu stehlen und Berechtigungen zu erweitern und so letztlich Zahlungskartendaten zu stehlen oder Ransomware-Angriffe zu starten.

SCHWACHSTELLEN-PATCHES

Kriminelle Akteure machen sich die Tatsache zunutze, dass IT- und Sicherheitsteams beim Patching ihrer POS-Systeme, E-Commerce-Zahlungsanwendungen sowie der zugrunde liegenden internen Infrastruktur kaum hinterherkommen. Um ihre Wettbewerbsfähigkeit aufrechtzuerhalten, investieren Händler in zusätzliche digitale Kanäle, Anwendungen und Technologien. Dadurch werden ihre Umgebungen jedoch komplexer und die Patching-Probleme noch größer. Häufig sind Unternehmensbürokratie und fehlende Cybersicherheitsexperten der Grund dafür, dass Patches nicht zeitnah implementiert werden.

GEORDNETERE SICHERHEITSABLÄUFE IN EINZELHANDEL UND GASTGEWERBE

Eine zuverlässige Bedrohungsdatenplattform liefert Einzelhändlern und Unternehmen aus dem Gastgewerbe den Kontext sowie die Möglichkeiten zur Priorisierung, die für fundiertere Entscheidungen, schnellere Erkennung und Reaktion sowie für die erweiterte Zusammenarbeit der Teams und Schulungen für fortlaufende Verbesserungen erforderlich sind. Sie müssen keine bestehenden Sicherheitsinfrastrukturen oder Abläufe ändern, da alle Tools und Technologien nahtlos mit der offenen Architektur von ThreatQ zusammenarbeiten.

MIT THREATQ MEHR ERREICHEN:

- **KONSOLIDIERUNG** aller Quellen für externe (z. B. R-CISC) und interne (z. B. SIEM) Bedrohungs- und Schwachstellendaten in einem zentralen Repository
- **AUSSORTIERUNG** nicht relevanter Informationen und einfache Navigation in enormen Mengen von Bedrohungsdaten zur Konzentration auf wichtige Ressourcen und Schwachstellen
- **PRIORISIERUNG** der Aspekte, die in Ihrer Umgebung am wichtigsten sind
- **PROAKTIVE SUCHE** nach böswilligen Aktivitäten, die Zahlungskartenbetrug, Denial-of-Service-Angriffe sowie andere Schäden für Kunden und Händler aufzeigen kann
- **KONZENTRATION** auf bekannte Sicherheitsschwachstellen, die derzeit aktiv ausgenutzt werden und die Vorschriften-Compliance und Sicherheitslage beeinträchtigen können
- **SCHNELLERE ANALYSE UND REAKTION** auf Angriffe gegen mehrere Ziele (z. B. POS-Systeme, E-Commerce-Anwendungen, neue digitale Kanäle und unterstützende Infrastruktur)
- **AUTOMATISCHE** Einbindung von Bedrohungsdaten in Erkennungs- und Reaktionstools

Fordern Sie eine Live-Demo für ThreatQ Platform und ThreatQ Investigations an: threatq.com/demo

[1] 2018 Thales Data Threat Report – Retail Edition (Thales Report zu IT-Sicherheitsbedrohungen 2018: Einzelhändler-Ausgabe) (https://www.thalesesecurity.com/2018/data-threat-report-retail)

[2] 2018 Thales Data Threat Report – Retail Edition (Thales Report zu IT-Sicherheitsbedrohungen 2018: Einzelhändler-Ausgabe) (https://www.thalesesecurity.com/2018/data-threat-report-retail)

[3] Cisco 2018 Security Capabilities Benchmark Study (Benchmark-Umfrage von Cisco zu Sicherheitsfunktionen 2018) (https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/retail-security-infographic.pdf)

[4] Symantec White Paper – Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust (Symantec-Whitepaper zu Cybersicherheit für Einzelhändler: Strategien zu Stärkung Ihres Unternehmens, Förderung von Innovationen und Aufbau von Kundenvertrauen) (https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf)

ÜBER THREATQUOTIENT™

ThreatQuotient hat sich das Ziel gesetzt, die Effizienz und Effektivität von Sicherheitsabläufen mithilfe einer bedrohungsbasierten Plattform zu verbessern. Durch die Integration der bestehenden Prozesse und Technologien eines Unternehmens in eine zentrale Sicherheitsarchitektur beschleunigt und vereinfacht ThreatQuotient die Untersuchungen sowie die Zusammenarbeit innerhalb von und zwischen Teams und Tools. Dank Automatisierung, Priorisierung und Visualisierung verringern die Lösungen von ThreatQuotient die Menge nicht relevanter Informationen und heben Bedrohungen mit hoher Priorität hervor, damit begrenzte Ressourcen ihren Schwerpunkt auf diese Gefahren legen können und bei Entscheidungen unterstützt werden. ThreatQuotient hat seinen Hauptsitz in Nord-Virginia (USA) sowie internationale Zweigstellen in Europa und im APAC-Raum. Weitere Informationen finden Sie unter https://threatquotient.com.

TQ_ThreatQ-for-Retail-and-Hospitality_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885