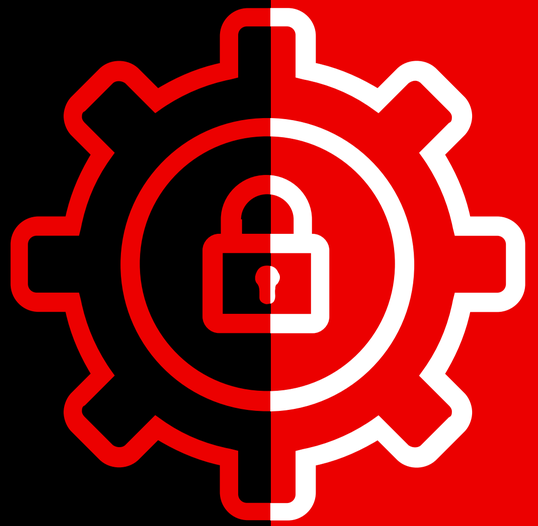
CROWDSTRIKE

Stoppen von Cyber-Bedrohungen im Finanzdienstleistungssektor

Folgen Sie in Zeiten eskalierender Cyber-Bedrohungen den Vorschriften, nicht den Angreifern



Die Wettbewerbs- und Betriebslandschaft für Finanzdienstleistungsunternehmen entwickelt und verändert sich. Die Nachfrage nach nahtlosen und personalisierten Erlebnissen schafft einen Bedarf an mehr Sicherheit und Datenschutz.

Hinzu kommt die Komplexität des exponentiellen Wachstums von daten- und cloudbasierten Systemen, wodurch Finanzdienstleistungsunternehmen zu einem Hauptziel für Cyberangriffe werden. Der Global Threat Report zeigt, dass die Zahl der Angriffe auf Finanzdienstleistungen jedes Jahr zunimmt.

Regulatorische Compliance ist nicht verhandelbar

Passen Sie sich schnell genug an, um Ihre Gegner zu überlisten?

Tun Sie genug, um den kommenden Vorschriften wie der EU-NIS2-Richtlinie und dem Digital Operational Resilience Act (DORA) Folge zu leisten?

Wenn Sie über die neuesten Trends im Bereich Cybersicherheit auf dem Laufenden bleiben, können Sie die operativen, finanziellen und rufschädigenden Folgen eines Angriffs vermeiden. Auf diese Weise entstehen auch keine hohen Bußgelder wegen Nichteinhaltung der Compliance-Vorschriften.

Strafen für Unternehmen des Finanzsektors, die sich nicht an die Vorschriften halten oder diese nicht melden:

10 Mio. €

bis zu 10 Mio. EUR oder 2 % des gesamten weltweiten Jahresumsatzes für NIS2.

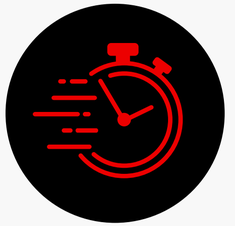
5 Mio. €

bis zu 5 Mio. EUR oder 2 % des gesamten weltweiten Jahresumsatzes für DORA.

▶ **Unsere Experten für Cybersicherheit können Ihnen bei der Orientierung bezüglich der neuesten regulatorischen Änderungen helfen.**

Was passiert in der Welt der Cybersicherheit und was bedeutet das für Finanzdienstleistungen?

7 WICHTIGE ERKENNTNISSE FÜR FINANZDIENSTLEISTUNGSUNTERNEHMEN AUS UNSEREM 2024 **GLOBAL THREAT REPORT**



1. Angriffe sind ausgefeilter und erfolgen schneller

Die Zeit, die benötigt wird, um auf ein Netzwerk zuzugreifen, hat sich drastisch reduziert:

- Die durchschnittliche Breakout-Zeit ist mit 62 Minuten um >25 % schneller als im Jahr 2023.
- Der schnellste aufgezeichnete Angriff betrug nur 2 Minuten 7 Sekunden.

WAS KÖNNEN SIE TUN?

Compliance

aktualisieren und testen Sie regelmäßig Pläne für die Reaktion auf Zwischenfälle, um die NIS2-Anforderungen für eine schnelle Ereignisberichterstattung und -verwaltung zu erfüllen.

Maßnahme

Beschleunigen Sie die Erkennung und Reaktion auf Bedrohungen mit fortschrittlichen Lösungen für die Endpunktbasierte Detektion und Reaktion (EDR).

- **Bringen Sie sich schnell auf den neuesten Stand. Vertrauen Sie auf eine auf den Angreifer fokussierte Technologie mit der schnellsten Erkennungszeit (getestet durch MITRE ATT&CK® Evaluierungen), die auf den Finanzdienstleistungssektor zugeschnitten ist.**

2. Malware und Angriffsmethoden entwickeln sich weiter

75 % der Angriffe sind jetzt malwarelos, verglichen mit 40 % im Jahr 2019.

Je besser die Bedrohungserkennung wird, desto mehr finden Gegner neue Wege, um die Sicherheit zu umgehen. Gestohlene Identitätsdaten und Social-Engineering-Angriffe erschweren die Erkennung von Kompromittierungen.

WAS KÖNNEN SIE TUN?

Compliance

Implementieren Sie strenge Zugriffskontrollen und überwachen Sie die Benutzeraktivität, um die NIS2-Anforderungen für die Sicherung von Netzwerk- und Informationssystemen zu erfüllen.

Maßnahme

Verbessern Sie den Identitätsschutz mit Multifaktor-Authentifizierung (MFA).

- **Nutzen Sie Threat Hunting-Dienste, um sich über neue Techniken von Angreifern auf dem Laufenden zu halten.**

3. Cloud-Kompromittierungen haben zugenommen

Cloudorientierte Angriffe sind innerhalb eines Jahres um **110 %** gestiegen.

Cyberangreifer nutzen Schwachstellen in der Cloud-Sicherheitskonfiguration aus, um den Cloud-Service des Opfers anzugreifen.

WAS KÖNNEN SIE TUN?

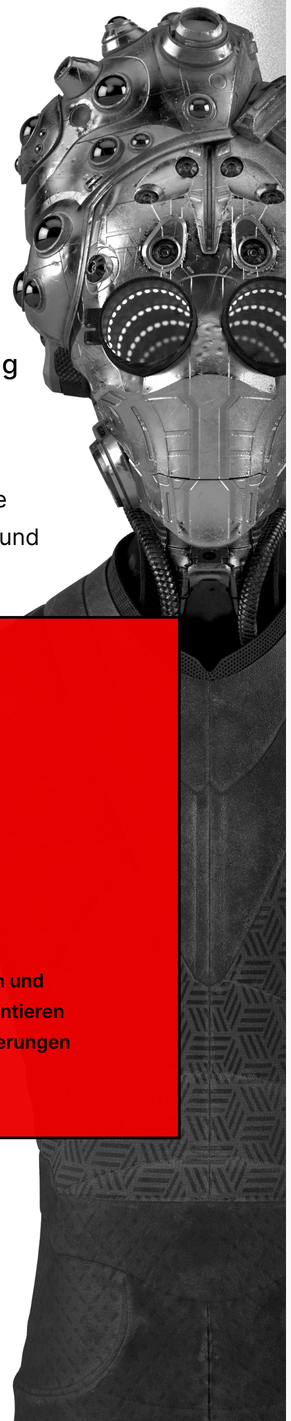
Compliance

Stellen Sie sicher, dass Cloud-Anbieter die NIS2-Standards und Best Practices einhalten, um cloudbasierte Daten und Services zu schützen.

Maßnahme

Führen Sie umfassende Cloud-Sicherheits-Frameworks ein, einschließlich Identitäts- und Zugriffsverwaltung (IAM), Verschlüsselung und kontinuierlicher Überwachung.

- **Warten Sie nicht, bis Angreifer Ihre Finanzsysteme kompromittieren. Beauftragen Sie Experten, um Angriffe zu verhindern.**



4. Beziehungen zu Dritten werden ausgenutzt

Kommerzielle Software aus dem Technologiesektor war der Ursprung der meisten kompromittierten vertrauenswürdigen Beziehungen.

Angreifer nehmen zunehmend Drittanbieter und Lieferketten ins Visier, um auf die Netzwerke von Finanzinstituten zuzugreifen, und nutzen dabei deren vernetzten und vertrauenswürdigen Charakter aus.

WAS KÖNNEN SIE TUN?

Compliance

Entwickeln und setzen Sie Risikomanagementrichtlinien für Drittanbieter durch, um die erweiterten NIS2-Anforderungen für die Sicherheit der Lieferkette zu erfüllen.

Maßnahme

Führen Sie strenge Sicherheitsprüfungen und Audits aller Drittanbieter durch. Implementieren Sie vertragliche Cybersicherheitsanforderungen für externe Anbieter.

▶ **Angreifer erzielen durch Angriffe über Beziehungen zu Dritten eine hohe Rendite. Stellen Sie sicher, dass die Sicherheitsstandards Ihrer Lieferanten und Anbieter genauso streng sind wie Ihre eigenen.**

5. Angreifer nutzen generative KI

KI kann für feindliche Informationsoperationen missbraucht werden, insbesondere wenn das Zielpublikum weniger digital versiert ist.

Generative KI hat die Eintrittsbarriere für ausgeklügelte und weit verbreitete Angriffe gesenkt.

WAS KÖNNEN SIE TUN?

Compliance

Aktualisieren Sie regelmäßig Cybersicherheitsstrategien, um neuen KI-Bedrohungen zu begegnen und den NIS2-Fokus auf proaktives Bedrohungsmanagement zu erfüllen.

Maßnahme

Bleiben Sie über KI-gesteuerte Bedrohungen auf dem Laufenden und erwägen Sie den Einsatz von KI-basierten Cybersicherheitstools, um fortschrittliche Techniken zu erkennen und ihnen entgegenzuwirken.

▶ **Nutzen Sie die transformative Kraft generativer KI in allen Sicherheits-Workflows, um Ihr Unternehmen zu schützen.**

6. Identitätsschutz muss oberste Priorität haben

In unserem Global Threat Report 2024 finden Sie Beispiele aus der Praxis, in denen Phishing und die Ausnutzung von Software-Schwachstellen das Sammeln von Anmeldeinformationen ermöglicht haben.

Identitäten sind ein Hauptziel für Cyberangriffe, wobei immer mehr Angreifer gestohlene Anmeldedaten nutzen, um sich unbefugten Zugang zu verschaffen.

WAS KÖNNEN SIE TUN?

Compliance

Übernehmen Sie Best Practices der Branche für die Identitäts- und Zugriffsverwaltung (IAM), wie wir sie bereits umsetzen, um die NIS2-Anforderungen zum Identitätsschutz zu erfüllen.

Maßnahme

Implementieren Sie robuste Lösungen für die Identitäts- und Zugriffsverwaltung (IAM), einschließlich Echtzeitüberwachung und Anomalieerkennung.

▶ **Übertreffen Sie moderne Bedrohungen mit einer einheitlichen Plattform, um identitätsbasierte Angriffe zu vermeiden.**

7. Zeiten für die Erkennung von Zwischenfällen und die Reaktion darauf müssen minimiert werden

Angreifer versuchen in der Regel, ihren Zugriff über den ursprünglichen Angriffspunkt hinaus auszudehnen, was im Durchschnitt etwa eine Stunde dauert. Sie können dann in nur wenigen Sekunden verheerende Schäden anrichten.

Eine schnelle Erkennung und Reaktion auf Cyber-Zwischenfälle sind von entscheidender Bedeutung. Verzögerungen können durch eine Kompromittierung verursachte Schäden verschlimmern.

WAS KÖNNEN SIE TUN?

Compliance

Entwickeln Sie Pläne zur Reaktion auf Zwischenfälle und testen Sie diese regelmäßig, um ein schnelles Handeln zu gewährleisten und die strengen NIS2-Meldefristen einzuhalten.

Maßnahme

Investieren Sie in fortschrittliche Überwachungs- und Analysetools, die Echtzeit-Sichtbarkeit in die Netzwerkaktivität liefern.

Die Einhaltung von Vorschriften ist nicht verhandelbar, insbesondere für Finanzinstitute. Ein Alleingang setzt Ihr Unternehmen – und Ihre Kunden – unnötigen Risiken aus.

Richten Sie ein spezielles Compliance-Team ein, um regulatorische Entwicklungen zu überwachen und sicherzustellen, dass Ihre Cybersicherheitspraktiken auf dem neuesten Stand sind. Stellen Sie sicher, dass sie regelmäßige Compliance-Audits durchführen und die Richtlinien aktualisieren, um sie an NIS2, DORA und andere relevante Frameworks anzupassen.

Experten für Cybersicherheit können Ihnen bei der Orientierung bezüglich der neuesten regulatorischen Änderungen helfen.

Lesen Sie unseren CrowdStrike Global Threat Report 2024

7 Die wichtigsten Erkenntnisse aus dem CrowdStrike Global Threat Report 2024

1. Angriffe sind ausgefeilter und erfolgen schneller
2. Malware und Angriffsmethoden entwickeln sich weiter
3. Cloud-Kompromittierungen haben zugenommen
4. Beziehungen zu Dritten werden ausgenutzt
5. Angreifer nutzen generative KI
6. Identitätsschutz muss oberste Priorität haben
7. Zeiten für die Erkennung von Zwischenfällen und die Reaktion darauf müssen minimiert werden

BERICHT HERUNTERLADEN

CROWDSTRIKE

Über CrowdStrike

CrowdStrike (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit einer der weltweit fortschrittlichsten cloudnativen Plattformen für Endgeräte- und Workloadschutz sowie Identität und Daten die Sicherheit geschäftskritischer Unternehmensbereiche neu.

Die CrowdStrike Falcon®-Plattform nutzt die CrowdStrike Security Cloud und erstklassige KI, um Echtzeit-Angriffsindikatoren, Threat Intelligence, sich entwickelnde Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform äußerst präzise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren.

CrowdStrike Falcon® wurde funktionsorientiert in der Cloud entwickelt und ermöglicht über einen einzigen schlanken Agenten schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite.

CrowdStrike: We stop breaches.