VMRAY

CYBER-RESILIENZ FÜR DEN FINANZSEKTOR

Mit modernernen Sandboxing-Technologien modernen Malware-Angriffen begegnen

Mit dem hohen Grad an Digitalisierung im Finanzsektor hat sich auch der Bankraub digitalisiert. Das Thema ist von großer Tragweite, denn ein erfolgreicher Cyberangriff auf einen Finanzmarktakteur bedeutet nicht nur Imageschaden und wirtschaftliche Einbußen für das betroffene Unternehmen: durch die enge Vernetzung können regelrechte Domino-Effekte entstehen, die im schlimmsten Fall die Funktionsfähigkeit der gesamten Finanzmarktinfrastruktur in Mitleidenschaft ziehen.

FINANZSEKTOR IM VISIER: VIELFÄLTIGE BEDROHUNGSLANDSCHAFT

Angreifer nutzen mittlerweile eine Vielzahl ausgeklügelter Vorgehensweisen, um die Sicherheitsvorkehrungen der Finanzinstitute auszuhebeln. Die Bandbreite reicht von Banking Trojanern und Überweisungsbetrug durch Spear-Phishing, über Ransomware und netzwerkbasierte Malware-Angriffe auf Geldautomaten bis hin zu Sabotage mithilfe von DDoS-Angriffen und Wiper-Attacken, die darauf abzielen, ganze Datenbestände zu löschen.

Die Finanzbranche zählt in allen Industrienationen zu den kritischen Infrastrukturen (KRITIS), deren Versorgungsdienstleistungen wichtig für das reibungslose Funktionieren des Gemeinwesens sind. Da wundert es nicht, dass die Finanzmarktbehörden die Unternehmen auffordern, einen kritischen Blick auf ihre Cybersicherheitskonzepte zu werfen.

REGULATORISCHE UND GESETZLICHE VORGABEN

Der europäische Finanzsektor unterliegt den strengen regulatorischen Vorgaben nationaler und internationaler Aufsichtsbehörden, die eine Erhöhung der Cyber-Resilienz im Finanzumfeld einfordern.

So empfiehlt die **European Banking Authority (EBA)** in ihren Leitlinien die Umsetzung eines **gestaffelten Sicherheitskonzepts (Defence-in-Depth)**. Hierbei sollen **Sicherheitsmaßnahmen (Controls) über mehrere Ebenen** eingeführt werden, die Personen, Prozesse und die Technologie umfassen. Jede Ebene dient dabei als Sicherheitsnetz für die vorhergehende Ebene. Der gestaffelte Ansatz soll zudem so verstanden werden, dass ein Risiko durch mehrere Sicherheitsmaßnahmen abgesichert wird, zum Beispiel durch Zwei-Faktor-Authentifizierung zusätzlich zu Netzwerksegmentierung und mehrfachen Firewalls.

Zudem sollen Finanzinstitute **Erkennungsmaßnahmen zur Feststellung möglicher Datenlecks, schädlichem Code und sonstiger Sicherheitsrisiken** sowie von öffentlich bekannten Schwachstellen von Software und Hardware einführen.

Neben den europäischen und nationalen Leitlinien verlangt zudem die **DSGVO (Europäische Datenschutz-Grundverordnung)** geeignete **Sicherheitsvorkehrungen im Umgang mit personenbezogenen Daten** und stellt bei Verstößen empfindliche Strafen in Aussicht.

Nationale Richtlinien in Deutschland, Österreich und der Schweiz

In **Deutschland** gibt die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in ihren **Mindestanforderungen an das Risikomanagement (MaRisk)** vor, dass für IT-Risiken angemessene Überwachungs- und Steuerungsprozesse einzurichten sind. Diese sollten insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und -minderung umfassen.

In **Österreich** gelten die Empfehlungen seitens der Finanzmarktaufsicht (FMA), die im **Leitfaden für IT-Sicherheit in Kreditinstituten** konkretisiert werden und den Leitlinien der European Banking Authority folgen. Der FMA-Leitfaden gibt unter anderem vor, dass Institute über angemessene Verfahren, Prozesse und technisch-organisatorische Maßnahmen verfügen sollten, um Daten vor Verlust und Beschädigung zu schützen. Gleiches gilt für den Schutz vor Malware, Datendiebstahl und Cyberkriminalität.

In der **Schweiz** gelten die Vorgaben der Eidgenössischen Finanzmarktaufsicht (FINMA). Cyberrisiken stehen dabei besonders im Fokus des **FINMA Rundschreibens RS 2008/21**, das eine zeitnahe Erkennung und Aufzeichnung von Cyberattacken fordert. Finanzinstitute müssen eine geeignete Aufbau- und Ablauforganisation konzipieren, um eine 24/7 Erkennung von Cyberattacken gewährleisten zu können.

BEST PRACTICES FÜR HOHE CYBER-RESILIENZ

Ausschlaggebend für eine hohe Cyber-Resilienz ist unter anderem das lückenlose Ineinandergreifen der verschiedenen Security-Maßnahmen. Diese sollten ein engmaschiges, mehrschichtiges System bilden, in dem eine Cyberbedrohung, falls sie einer Security-Instanz entgeht, von einer anderen aufgehalten wird. Zu den gängigsten Komponenten eines solch mehrschichtigen Systems gehören Firewalls, Endpoint-Security-Lösungen, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Email- und Web-Gateways, Verfahren zur Zugangs- und Berechtigungskontrolle, aber auch Konzepte wie Netzwerksegmentierung. Eine weitere wichtige Komponente sind Sandboxing-Technologien. Sie spielen eine entscheidende Rolle, wenn es um die Erkennung und Analyse von Advanced Malware geht. Unter diesem Oberbegriff werden unterschiedliche Typen von Malware zusammengefasst: dazu gehören bislang unbekannte Bedrohungen (Zero-Day Malware), hochentwickelte, evasive Malware (z.B. polymorphe und metamorphe Malware) sowie komplexe, zielgerichtete Angriffe (z.B. politisch motivierte Attacken). Diese Bedrohungen sind mit anderen Sicherheitskomponenten nicht zu erkennen.

WAS EINE SANDBOX KÖNNEN SOLLTE

In einer Sandbox werden verdächtige Dateien in einer abgesicherten Umgebung ausgeführt und analysiert. Falls sich die Datei als Malware herausstellt, kann das Security Team umgehend die Systeme gegen die neu erkannte Gefahr härten. Sandboxing-Lösungen sind fester Bestandteil einer jeden ausgereiften Cybersecurity-Architektur. Doch nicht immer erfüllt die eingesetzte Sandbox die Erwartungen der SOC- und IR-Teams (SOC und Incident Response). Die Gründe können in einer unbefriedigenden Erkennungsrate liegen, mit zu vielen False Positives (unnötige Fehlalarme) oder zu vielen False Negatives (Malware gelangt ins Firmennetz). Auch entspricht die Qualität der Analyse-Reports häufig nicht den Anforderungen oder es fehlen Automatisierungsfunktionen, um die Erkennungs- und Analyseprozesse effizienter zu gestalten.

Eine Sandboxing-Lösung, die den hohen Anforderungen im Finanzsektor genügen soll, muss daher die folgenden Kriterien erfüllen:

HOHE RESISTENZ GEGEN SANDBOX EVASION

- Viele gängige Sandboxing-Methoden hinterlassen in der Analyse-Umgebung deutliche Zeichen, die moderne Malware erkennen lässt, dass sie unter Beobachtung steht. Die Schadsoftware wird nun versuchen, durch Vortäuschen harmlosen Verhaltens der Entdeckung zu entgehen (Sandbox Evasion). Den Verschleierungstaktiken der Malware kann durch den Einsatz einer innovativen, Hypervisorbasierten Sandbox begegnet werden. Hier erfolgt die Beobachtung von außerhalb der Analyse-Umgebung (aus der Hypervisor-Schicht heraus) und bleibt für die Schadsoftware unsichtbar. So entfalten sich Angriffe in der Sandbox, die sich normalerweise der Erkennung entziehen würden. Um zielgerichtete Angriffe aufzudecken, die nur auf den Rechnern des anvisierten Finanzinstituts aktiv werden und deshalb nach entsprechenden Merkmalen suchen, ist es erforderlich, die reale Umgebung so detailgetreu wie möglich nachzubilden. Die Sandbox sollte deshalb in der Lage sein, Golden Images mit der Standard-Konfiguration des Unternehmens zu nutzen und mithilfe von Geo-Location-Einstellungen Unternehmensrechner in unterschiedlichen Ländern zu simulieren.

ELIMINIEREN VON HINTERGRUNDRAUSCHEN UND FEHLALARMEN

- Ausgefeiltes Monitoring und hohe Report-Qualität sind weitere essenzielle Kriterien bei der Wahl einer Sandbox-Lösung. Ein Analyse-Report muss einen granularen Einblick in die Aktionen und das Verhalten einer suspekten Datei ermöglichen, darf dabei aber kein irrelevantes Hintergrundrauschen aus der Systemumgebung beinhalten. Oft sind Reports zu oberflächlich und lückenhaft, d.h. es fehlten essenzielle Informationen über die Interaktionen der Malware mit dem Zielsystem oder aber das genaue Gegenteil ist der Fall - die Informationen sind zwar vorhanden, sie sind jedoch zwischen dem ebenfalls dokumentierten legitimen Hintergrundrauschen des Systems nur mit Mühe zu erkennen. Ein Beispiel: wird bei einer Malware-Analyse ein Microsoft Word-Dokument unter die Lupe genommen, dann sollten die gerechtfertigten Interaktionen der Anwendung mit der Systemumgebung keinesfalls im Report erscheinen. Je nach Sandbox kann das Signal-Rausch-Verhältnis jedoch bis zu 1:100 betragen. Werden Nutzsignale durch Rauschen in solchem Ausmaß verwässert, wird es sehr schwierig, Angriffsvektoren aufzudecken.

AUTOMATISIERUNG VON ERKENNUNGS- UND ANALYSEVORGÄNGEN

- Entlastung der SOC- und IR-Teams sowie Effizienzgewinn durch Prozessautomatisierung sind weitere wichtige Kriterien in Zeiten von Fachkräftemangel und dünner Personaldecke. Automatisierte Erkennungsprozesse sind skalierbar, sodass auch Teams mit geringer Personalstärke den stetigen Anstieg im Malwareaufkommen bewältigen können. Dabei sollte sich die Automatisierung auch auf die Extraktion zuverlässiger IoCs (Indicators of Compromise) aus der Masse forensischer Daten erstecken, denn in vielen Security Teams werden IoCs immer noch manuell generiert – ein zeitaufwändiger Vorgang, der erfahrene Threat Analysten voraussetzt.

GENERIERUNG UND BEREITSTELLUNG VON THREAT INTELLIGENCE

- Die Sandboxing-Lösung sollte darüber hinaus in der Lage sein, hochpräzise, zuverlässige Bedrohungsinformationen (Threat Intelligence) zu generieren und in der vorhandenen Security-Umgebung bereitzustellen, um beispielsweise Blockierungen von Endpoints und andere Sicherheitsmaßnahmen auszulösen. Um die Integration in die Security-Umgebung zu vereinfachen, sollte eine Vielzahl von Out-of-the-Box Konnektoren zur Verfügung stehen.

UNTERSTÜTZUNG VON COMPLIANCE-VORGABEN ZUR DATENHALTUNG

- Compliance-Anforderungen spielen insbesondere bei Cloud-basierten Sandboxing-Technologien eine Rolle, denn Bedrohungsdaten können auch direkten oder indirekten Personenbezug aufweisen. Dies ist besonders wichtig für Unternehmen in regulierten Branchen, die verpflichtet sind, die Kontrolle darüber zu haben, wo ihre Daten gespeichert werden. Die Nutzung DSGVO-konformer Rechenzentren innerhalb der EU ist deshalb ein weiterer Punkt, der bei der Wahl einer Sandboxing-Lösung beachtet werden sollte.

VMRAY

FAZIT

Die komplexe Cyberbedrohungslage kann nur beherrscht werden, wenn Incident-Response-Abteilungen und Security Operation Center ihre Maßnahmen zur Erkennung und Abwehr von Angriffen optimieren können. Dies wird deutlich durch die Ergebnisse der Untersuchung „Improving the Effectiveness of the Security Operations Center" des Ponemon-Institutes: Mehr als die Hälfte der Befragten (53 Prozent) bewertet die Fähigkeit ihres SOCs, Beweise zu sammeln, Nachforschungen anzustellen und die Quelle von Bedrohungen zu finden, als ineffizient. Die SOC-Teams haben Schwierigkeiten, Bedrohungen zu identifizieren, weil sie zu viele Indicators of Compromise (IOCs) verfolgen müssen, zu wenig interne Ressourcen und Know-how zu Verfügung stehen und zu viele Fehlalarme auftreten.

Der Einsatz einer geeigneten Sandboxing-Lösung als Spezialwerkzeug zur Erkennung und Analyse von Advanced Malware gewinnt in diesem Zusammenhang umso mehr an Bedeutung.

Die VMRay Plattform umfasst drei Lösungen, die auf spezifische Incident Response- und SOC-Anforderungen ausgerichtet sind:

VMRAY ANALYZER

Der Gold Standard für die dynamische Analyse moderner Malware liefert Bedrohungsinformationen in großer Detailtiefe und unterstützt IR-Teams bei der Erkennung komplexer Angriffe.

VMRAY ETD

Ergänzt vorhandene Email-Security-Lösungen und identifiziert Email-basierte Angriffe, die von anderen Systemen nicht erkannt und abgefangen werden.

VMRAY DETECTOR

Skaliert die automatisierte Erkennung von Malware über das gesamte Unternehmen hinweg und stellt schnelle, präzise Verdikte zum Schadpotenzial der untersuchten Malware-Samples bereit.

ÜBER VMRAY

VMRay bietet die branchenweit präziseste Lösung zur automatisierten Erkennung und Analyse moderner Malware-Bedrohungen. VMRay schließt Lücken in der vorhandenen Security-Umgebung des Unternehmens und wehrt Bedrohungen ab, die von anderen Sicherheitslösungen nicht erkannt werden.

Weltweit vertrauen Unternehmen und Organisationen mit hohen Cybersicherheitsanforderungen auf VMRay Technologien. Zum Kundenkreis zählen global agierende Finanz- und Versicherungsunternehmen, Industrie- und Technologiekonzerne, führende Wirtschaftsprüfungsunternehmen, sowie Behörden, Regierungs- und Forschungseinrichtungen.

VMRAY