FINANZIERUNG
LEASING
FACTORING
FLF

4

JULI 2024 · 71. JAHRGANG

Foto: Gerd Altmann/pixabay

DIGITALER SONDERDRUCK

DIGITALISIERUNG

Cyber Security: Managed Detection and Response

Auf Bedrohungen richtig reagieren

Simon Hanke, Cyber Defense Consultant, SECUINFRA GmbH

Cyber Security: Managed Detection and Response

Auf Bedrohungen richtig reagieren

Cyber-Bedrohungen stellen in der Finanzbranche mittlerweile eines der größten Risiken dar. Zahlreiche aktuelle Studien belegen, dass Banken, Versicherungen und Finanzdienstleister zunehmend ins Visier von Cyber-Angreifern geraten. An erster Stelle der Bedrohungen stehen nach wie vor Business-E-Mail Compromise, Ransomware-Attacken sowie Angriffe auf die Supply Chain, also etwa auf Drittanbieter oder die (Cloud-)Infrastruktur. In seinem Beitrag geht der Autor auf das Managed Detection & Response (MDR) und dessen Bedeutung für Unternehmen ein. (Red.)

Die Konsequenzen können für die betroffenen Unternehmen gravierend sein und von der Weitergabe vertraulicher Informationen bis hin zur Unterbrechung ihres Kerngeschäfts reichen. Aus diesem Grund arbeiten die meisten Unternehmen aus der Finanzbranche bei der Abwehr von Cyber-Threats bereits mit hochspezialisierten Experten zusammen. Kein Wunder, denn die IT-Landschaft wird ständig komplexer, während die Zahl der Bedrohungen stetig steigt. Um dieser dynamischen Bedrohungsentwicklung effektiv zu begegnen, setzen viele Banken, Leasing-Anbieter und Factoring-Institute vermehrt auf spezialisierte MDR-Dienstleister. So kann eine aktive, schnelle und umfassende Gefahrenerkennung, -analyse und -abwehr dauerhaft gewährleistet werden – eine Aufgabe, die viele Finanzdienstleister sonst an ihre Grenzen brächte. Doch was ist das Besondere an MDR und wie unterscheidet es sich von inhouse betreuten IT-Security-Systemen?

Foto: SECUINFRA GmbH; Peter Venus (capitalheadshots)

SIMON HANKE

ist Cyber Defense Consultant
bei SECUINFRA GmbH, Fankfurt am Main.

E-Mail:
simon.hanke@secuinfra.com

Umfassende Abwehr von Cyber-Gefahren

Bei Unternehmen aus dem Finanzbereich besitzen die eigenen IT-Teams meist weder die Expertise noch die notwendigen Ressourcen, um Cyber-Bedrohungen effizient zu erkennen und zu stoppen. Aufgrund umfangreicher administrativer Tätigkeiten ist die Betreuung der IT-Security in vielen Instituten nur eine von vielen Aufgaben der IT. Bei der akuten Bedrohungslage kann dies jedoch fatale Auswirkungen haben.

Das Security-Monitoring als Managed Service bietet hingegen eine Rund-um-die-Uhr-Überwachung auf hochprofessionellem Niveau, welches mit dem eigenen IT-(Security)-Team einen unverhältnismäßig hohen Aufwand an Zeit und Budget bedeuten würde. Die Expertenteams der Dienstleister sind auf die Überwachung der IT-Systeme und die Erkennung und Analyse von IT-Sicherheitsvorfällen spezialisiert. Bemerken sie eine akute Bedrohung, können sie diese umgehend isolieren und ihre Auswirkungen eindämmen. Dazu bringen MDR-Dienstleister eigene Software-Lösungen mit, die an die Kundenumgebung angepasst werden. Um die Lizenzierung und die technischen Details des Einsatzes dieser Tools muss sich der Kunde keine Gedanken mehr machen, was für viele Finanzinstitute eine große personelle und finanzielle Entlastung darstellt.

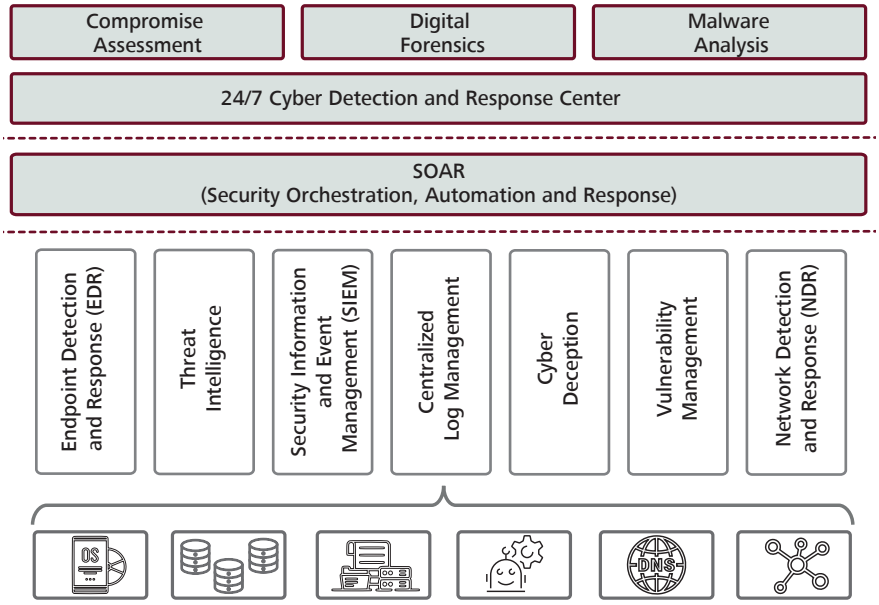
> »Die Betreuung der IT-Security ist in vielen Instituten nur eine von vielen Aufgaben der IT.«

Managed Detection & Response ist eine umfassende Sicherheitsdienstleistung, die darauf ausgerichtet ist, Cyber-Bedrohungen zu erkennen, auf sie zu reagieren und sie zu neutralisieren. Im Gegensatz zu herkömmlichen IT-Dienstleistungen, bietet MDR einen ganzheitlichen Ansatz, um Unternehmen aus der Finanzbranche vor, während und nach einem Sicherheitsvorfall zu unterstützen. Dabei punktet MDR mit einer großen Auswahl an verschiedenen Überwachungsmodulen sowie deren Zusammenspiel. Somit sind die Kunden von MDR-Dienstleistungen bestmöglich vor Cyber-Gefahren geschützt, ohne intern massiv in Know-how und Personal investieren zu müssen.

Technische Basis

Das Herzstück eines MDR-Service bildet typischerweise das Security Information & Event Management (SIEM). Zur logbasierten Angriffserkennung verarbeitet es sämtliche relevanten Log-Daten des

Abbildung 1: Modular aufgebautes MDR-Angebot mit Basis-Komponenten, SOAR und Monitoring-Services



Quelle: SECUINFRA

Unternehmens. Zudem dient es als zentralisiertes Log-Management und die Speicherung aller relevanter Informationen über einen längeren Zeitraum. Ergänzt wird die logbasierte Angriffserkennung durch Alarme von EDR-Systemen (Endpoint Detection & Response), welche Ereignisse direkt auf den Endgeräten erkennen und unterbinden, sowie von NDR-Systemen (Network Detection & Response), die diese Aufgaben im Netzwerkbereich übernehmen. Die zuletzt genannten Systeme werden im Security Bereich auch als XDR (Extended Detection & Response) bezeichnet.

Als weitere Bestandteile des technischen Fundaments wird auf Basis von Threat Intelligence Feeds nach bekannten Indicator of Compromise (IoC) sowie verdächtigen Aktivitäten in den Datenquellen gesucht. Zudem versucht die Cyber Deception durch die bewusste Platzierung von Dummy-Accounts oder anderen Informationen in der Unternehmensinfrastruktur, Angreifer durch Täuschungsmanöver von den eigentlichen Kronjuwelen im Unternehmensnetzwerk abzulenken und Hacker in die Falle zu locken. Präventiv kann ein Baustein für Vulnerability-Management Schwachstellen in der IT-Infrastruktur durch zyklische Scans und Analysen systematisch aufdecken und somit widerstandsfähiger machen.

Um alle Ereignisse und Alarme im Überblick zu behalten, nutzen Security Analysten eine SOAR-Lösung (Security Orchestration Automation and Response). SOAR bietet die Möglichkeit, eingehende Alarme aus unterschiedlichen IT-Sicherheitssystemen wie SIEM, EDR oder NDR innerhalb des Unternehmens zentralisiert und effizient zu bearbeiten. Dazu sind an das SOAR-System neben allen Alarmquellen auch Tools zur Informationsgewinnung angebunden. Zudem können bestimmte Analysetätigkeiten und Response-Maßnahmen anhand von zuvor definierten Playbooks automatisch durchgeführt werden.

24/7 Abwehr durch Cyber-Defense-Experten

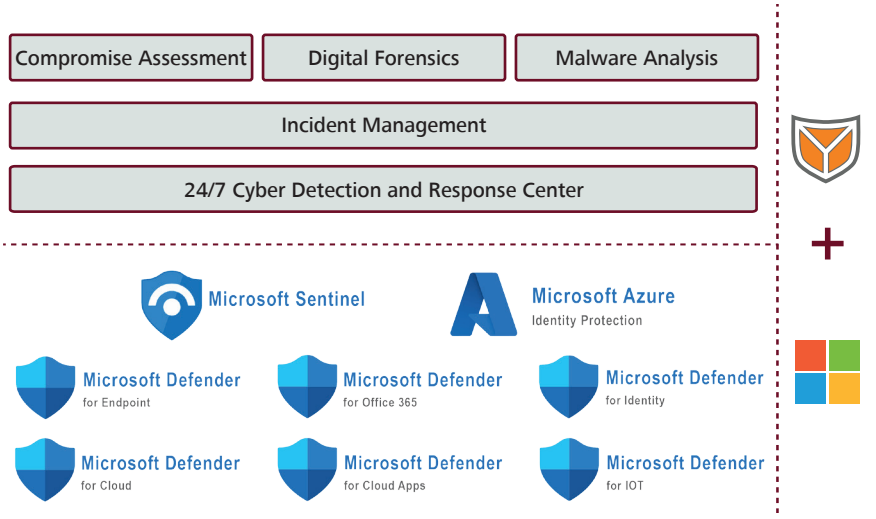
Einen Cyber-Angriff zu erkennen und zu analysieren, ist eine Sache. Eine andere ist es, ihn so schnell wie möglich professionell abzuwehren. Für einen effektiven Schutz benötigt man deshalb auch eine gehörige Portion menschliches Know-how als entscheidende Ergänzung zu automatisierten Response-Technologien, wie sie von EDR, NDR und SOAR bereitgestellt werden. Erst in Kombination mit der Expertise erfahrener Cyber-Defense-Analysten, die in den unterschiedlichsten Sicherheitsbereichen zu Hause und rund um die Uhr im Einsatz sind, entfaltet MDR sein volles Potenzial. So können im richtigen Moment beispielsweise kompromittierte Konten gesperrt, infizierte Systeme vom Netz genommen oder andere im Incident-Response-Plan vereinbarte Maßnahmen ergriffen werden.

Die notwendigen Alarme und Informationen für ein rechtzeitiges und angemessenes Handeln erhalten die MDR-Spezialisten aus ihrem Werkzeugkasten mit SIEM, EDR, NDR, Threat Intelligence und Cyber Deception. Alle Meldungen fließen in das SOAR-System ein, wo viele Prozesse bereits automatisiert ablaufen. Ergänzend dazu werten die Sicherheitsexperten die erkannten Ereignisse aus und reagieren entsprechend. Im Rahmen eines professionellen Incident Managements werden zudem Malware-Analysen durchgeführt, um potenzielle

Auswahlkriterien für einen MDR-Dienstleister

Die Zusammenarbeit mit einem MDR-Dienstleister bietet Kreditunternehmen, Banken und anderen Finanzinstituten die Möglichkeit, einen umfassenden Cyber-Sicherheitsansatz zu implementieren, der über die internen Kapazitätsgrenzen hinausgeht. Welcher MDR-Dienstleister infrage kommt, hängt von der Unternehmensgröße und der vorhandenen Sicherheitslandschaft ab. Auch die Personalstärke und Security-Expertise des eigenen IT-Teams sowie die zu berücksichtigenden Compliance-Vorschriften sind in die Anbieterentscheidung miteinzubeziehen. Für die Anbieterauswahl gilt es neben dem Nachweis von Expertise und Branchenerfahrung darauf zu achten, dass dieser im Notfall schnell reagiert, transparent und regelmäßig berichtet und dass das Preis-Leistungsverhältnis zum erwartbaren Schutzniveau passt.

Abbildung 2: Cloud-Lösung – proaktiver Schutz von Cloud und Endgeräten mit Microsoft



Quelle: SECUINFRA

oder bestätigte Schadsoftware möglichst umfassend zu verstehen und die Abwehr zu optimieren.

Sollte es dennoch zu einem Sicherheitsvorfall gekommen sein, kann ein zeitnahes Compromise Assessment betroffene Systeme anhand von Indicator of Compromise (IoCs) identifizieren und für eine tiefgreifende Untersuchung priorisieren. Für die detaillierte Untersuchung nutzen die Spezialisten forensische Methoden, um Cyber-Sicherheitsvorfälle zu untersuchen und zeitnah geeignete Gegenmaßnahmen einzuleiten. So können sie akute Schäden effektiver minimieren und die Arbeitsfähigkeit schnellstmöglich wiederherstellen.

Flexibler Einsatz in drei Varianten

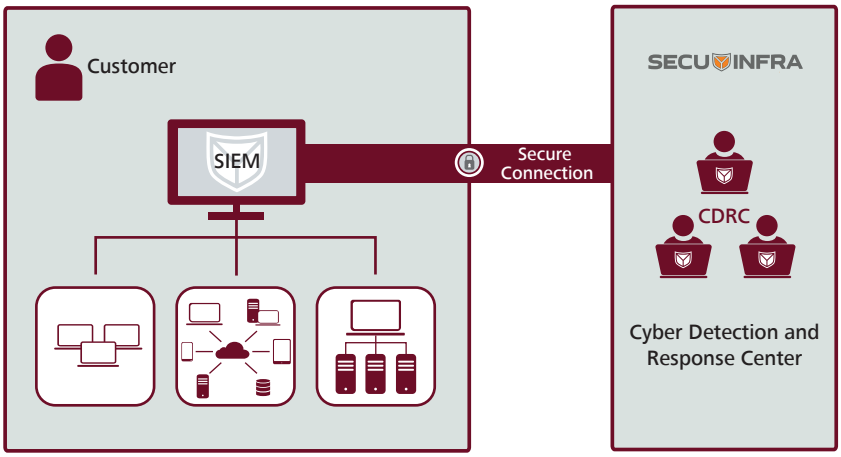
MDR-Dienstleistungen sind also schlüsselfertige Gesamtlösungen, die auf die bekannten Anforderungen zum Beispiel der Kreditwirtschaft oder der Leasing-Branche zugeschnitten sind. Dabei sind Lösungen etwa unter Einbeziehung der Microsoft Cloud auf Basis der Defender-Produktfamilie genauso möglich wie auf Basis von Lösungen, die ohne Cloud auskommen und entsprechenden Datenschutzansprüchen gerecht werden. Letzteres ist besonders für diejenigen Unternehmen wichtig, die keine Cloud-Systeme einsetzen möchten oder dürfen.

Bei Firmen, die bereits Microsoft im Einsatz haben und auf die Cloud setzen, bietet es sich hingegen an, darauf aufzubauen. In diesem Fall werten externe Security-Spezialisten die Daten von Microsoft Sentinel und Microsoft Defender aus. Dies dient der Erkennung, Analyse und Abwehr von Bedrohungen auf Endgeräten sowie in Multi- und Hybrid-Cloud-Systemen. Neben der Datenanalyse setzen die Experten weitere Tools und Techniken ein, um Anomalien und potenzielle Sicherheitsrisiken zu identifizieren. Hierbei ist ein hohes Maß an Kenntnis der neuesten Microsoft-Technologien erforderlich. In der Regel findet daher eine enge Zusammenarbeit mit Microsoft statt. Auf diese Weise kann der MDR-Dienstleister seine Kunden frühzeitig über Updates und Neuerungen informieren, proaktiv agieren und bestmöglichen Schutz vor sich ständig verändernden Bedrohungen bieten.

Es gibt allerdings viele Finanzdienstleister, die etwa aus Datenschutzgründen keine Cloud einsetzen oder diesbezüglich Vorbehalte gegen einen amerikanischen Softwareanbieter haben. Auch in diesem Fall ist ein externe MDR-Service möglich, der dann beispielsweise auf Open-Source und inhouse gehostete Lösungen aufbaut. Dabei verbleiben alle Daten in der Infrastruktur des Dienstleisters. Die Angriffserkennung findet durch eine logbasierte (SIEM), endpointbasierte (EDR) und netzwerkbasierte (NDR) Analyse statt. Die Erkennungsregeln sogenannter Use Cases stammen dabei vom Dienstleister, der auf dessen Entwicklung spezialisiert ist und das benötigte Know-how mitbringt.

Zudem können Erkennungsregeln auf Basis von Maschine Learning mithilfe der im SIEM vorhandenen Module die Alarmierung ergänzen. Abgerundet wird das Angebot des MDR-Dienstleisters durch die Analyse von Threat Intelligence

Abbildung 3: Co-Managed SIEM – über eine gesicherte Verbindung greifen die Security-Experten auf das SIEM-System des Finanzunternehmens zu



Quelle: SECUINFRA

Feeds und die implementierten Cyber-Deception-Maßnahmen.

Sollten größere Banken oder Kreditinstitute bereits Cyber-Defense-Produkte im Einsatz haben, kann ein externer MDR-Dienstleister dennoch sehr nützlich sein. Dieser kann etwa beim 24/7-Betrieb unterstützen oder helfen, die eingesetzten Module optimal an das Unternehmen anzupassen und zu erweitern. Beim Co-Manged SIEM oder Co-Managed XDR verbleiben alle Komponenten und Daten im Besitz des Unternehmens. Gleiches gilt für die Erkennungsmechanismen, die geistiges Eigentum des jeweiligen Finanzinstituts bleiben. Dies ermöglicht eine volle Kontrolle und jederzeit problemlose Anpassungen im laufenden Betrieb. Je nach Aufgabenstellung sitzen die externen Cyber-Defense-Experten entweder direkt beim Finanzdienstleister vor Ort oder greifen über eine gesicherte Verbindung auf die Security-Tools zu. Im regelmäßigen Austausch stimmen sich die eigenen Security-Experten mit dem Dienstleister über die Security Prozesse und erforderlichen Maßnahmen ab.

In allen Fällen bringt das Einbeziehen eines externen MDR-Service viele Vorteile mit sich. Auf diese Weise sparen sich Finanzinstitute nämlich strategische und taktische Überlegungen zur Auswahl von Software und Detektionsmechanismen sowie die Ausgestaltung der erforderlichen Prozesse. Dennoch bedarf es auch in diesem Fall eines stetigen Austausches zwischen Dienstleister und Kunden. Trotz der Auslagerung des Großteils der Arbeit baut der Kunde so im Laufe der Zusammenarbeit eine gewisse Kompetenz im Umgang mit (potenziellen) Sicherheitsvorfällen auf, da er in kritische Entscheidungsprozesse stets miteinbezogen wird.

Nahtlose Integration, laufender Austausch

Zusammenarbeit ist auch das Stichwort für die abschließende Fragestellung: Wie sieht die Kooperation mit einem MDR-Dienstleister konkret aus? Für eine lückenlose Integration der relevanten MDR-Tools und -Prozesse müssen Dienstleister und IT-Teams Hand in Hand zusammenarbeiten. Schließlich ist es wichtig, dass die spätere Cyber-Abwehr schnell und reibungslos ablaufen kann. Dazu zählt eine klare Definition der Aufgaben und Analysetätigkeiten genauso wie eine Abgrenzung der möglichen Reaktionsmaßnahmen, um den operativen Betrieb nicht unnötig zu stören. Gerade Letzteres ist beispielsweise für Finanzdienstleister von entscheidender Bedeutung. Zudem sind regelmäßige Besprechungen und Updates empfehlenswert, damit beide Seiten stets über die aktuelle Sicherheitslage und mögliche Herausforderungen informiert sind. Gleichwohl sollte nicht vergessen werden, dass jedes Unternehmen einzigartig ist, weshalb MDR-Anbieter ihre Dienstleistungen unbedingt auf die kundenspezifischen Anforderungen und Ziele abstimmen müssen.

»Es gibt viele Finanzdienstleister, die aus Datenschutzgründen keine Cloud einsetzen.«

Die zunehmende Notwendigkeit, auf Bedrohungen zu reagieren, macht ausgelagerte Managed Detection and Response (MDR) Services für Unternehmen aus der Finanzbranche immer attraktiver. Denn mithilfe dieser fortschrittlichen Cyber-Sicherheitsdienstleistung lässt sich das Schutzniveau zu kalkulierbaren Kosten auf Unternehmensebene anheben, was ansonsten intern kaum darstellbar ist. Mit einem erfahrenen MDR-Partner, der die aktuelle Cyber-Bedrohungslandschaft kennt und die notwendigen Ressourcen für eine 24/7-Abwehr bereitstellt, können Finanzdienstleister jeder Größe daher gut gerüstet in die digitale Zukunft blicken.