USE CASE

SIEM plus AI-Security

Event statt eventuell: Alarm schon auf Verdacht!

Projektumfeld

IT-Sicherheit ist mittlerweile ein Thema von volkswirtschaftlicher Relevanz. So gehen allein in Deutschland über 50 Milliarden Euro an Kosten jährlich aufs Konto von Cyberkriminalität. Und herkömmliche Sicherheitsvorkehrungen wie Firewalls, Antiviren-Tools, HTTPS-Protokolle oder SSL-Scanning sind beispielsweise gegen systematisch geplante Attacken kein zuverlässiger Schutz mehr. Ehe sie zuschlagen, dringen Angreifer heute schon Wochen zuvor in das Netzwerk ein und spähen dort mögliche Ziele in aller Ruhe aus. 100-prozentige Sicherheit dagegen ist eine Illusion. Klarheit, und damit auch alle Optionen zur Abwehr, bringt hier nur vorausschauend strategisches Handeln in Form des rechtzeitigen Erkennens! In diesem konkreten Fall praktiziert bei einem deutschen Kreditinstitut. Durch ein erstes Beratungsgespräch erhielt Axians einen Einblick in zwei zentrale Faktoren für die Sicherheitsarchitektur: Zum einen die spezifischen Ansprüche des Kunden, zum anderen die Anforderungen der Finanzaufsicht. Vor allem Letztere zwingen die Bank praktisch dazu, permanent ihre Systeme, Netzwerke und Anwendungen im Hinblick auf Veränderungen oder Unregelmäßigkeiten zu überwachen.

Projektanforderungen & Projektziele

Eine wesentliche Anforderung an die IT im Finanzsektor ist das lückenlose Überwachen der Log-Informationen des Netzwerks und aller Applikationen. Logdateien protokollieren die Aktionen sämtlicher Prozesse im System. Dazu musste Axians zuerst neben der Aufnahme aller Sicherheitsvorgaben auch die entsprechenden Schnittstellen des Kunden definieren. Im näheren Fokus stehen dabei alle Tätigkeiten der administrativen User. Im erweiterten Aktionsradius geht es um Anomalien im Netz und das Erkennen von Szenarien wie etwa Attacken durch WannaCry oder anderen Schadcode. Die Lösung der Wahl für alle Aspekte hieß SIEM. Dieses Kürzel steht für „Security Information & Event Management". SIEM setzt Daten verschiedener Logquellen in Beziehung zueinander, um damit sogenannte „Events" zu identifizieren. Jedes Event wird dann hinsichtlich seines Risikopotentials taxiert. Sollte Gefahr im Verzug sein, wird nicht nur Alarm ausgelöst, sondern auch ein definierter Abwehrplan gestartet. Im Speziellen lag bei diesem Projekt eine Herausforderung in der neuen IT Umgebung des Kunden. Dort gibt es drei Stränge für Test, Pre-Produktion und Produktion, die alle in Bezug auf IP / MAC-Adressen und Informationsquellen identisch sind. In der Konsequenz muss das SIEM hier Mandantenfähig sein, um die Umgebungen sauber voneinander trennen zu können. Ferner ist es im Bankenumfeld nicht unüblich, im internen Netz öffentliche IP-Adressbereiche zu nutzen, was eine Modellierung des Netzwerks und der kritischen Anwendungen im SIEM umfangreicher gestaltet. Denn in diesem Fall lassen sich die konventionellen Regeln des SIEM-Systems zum Erkennen von Anomalien nicht oder nur in Teilen anwenden.

Umsetzung

Für die Anforderungen der Bank wurde nicht nur ein SIEM Produkt benötigt, sondern auch ein sensibel abgestimmtes Konzept – und damit alles andere als eine Lösung „von der Stange". Prozesse und Dokumentationen wurden durch Axians in enger Abstimmung mit dem Kunden entworfen. Immer unter der Prämisse, dass alles optimal mit der künftigen Betriebssituation harmoniert. Eine

NUTZEN

- Professionelles Security Information & Event Management durch ausgewiesene Cyber Threat Analysten
- Überwachte Infrastruktur rund um die Uhr
- Frühzeitiges Erkennen externer und interner Bedrohungen durch Echtzeit-Analyse
- Laufende Weiterentwicklung des Schutzschirms vor Angriffsszenarien durch Pentester und Analysten
- Einhaltung von Auflagen und Compliance-Anforderungen
- Wöchentliches Reporting, bedarfsgerechte Anpassungen

ÜBER AXIANS

Axians in Deutschland ist ein agiles Unternehmensnetzwerk aus spezialisierten ICT-Dienstleistern und Softwareherstellern unter der globalen ICT-Marke Axians der VINCI Energies. Durch eine flächendeckende Präsenz in 24 Städten existiert eine unmittelbare Nähe zum Kunden. Das Netzwerk begleitet seine Kunden – privatwirtschaftliche Unternehmen, kommunale Verwaltungen, öffentliche Einrichtungen, Netzbetreiber und Service Provider – während der gesamten ICT-Prozesskette. Die Kernkompetenzen aus IT-Lösungen, IT-Sicherheit, Netzwerkinfrastruktur und Netztechnik werden durch eigene Branchensoftware ergänzt und unterstützen den Kunden bei allen Anforderungen der Core-ICT und der digitalen Transformation. Durch die Kombination aus Beratung, Implementierung, Service und Betrieb können Kunden Technologien und Applikationen genau nach Bedarf nutzen, Prozesse optimieren und ihre digitalen Geschäftsstrategien zukunftssicher umsetzen. Mit 1.700 Spezialisten stellt Axians in Deutschland für jede Herausforderung eine individuelle Lösung mit dem besten Team aus dem Netzwerk bereit.

USE CASE

SIEM plus AI-Security

wichtige Schlüsselstelle ist der Informations-eigentümer einer zu überwachenden Anwendung. Technisch gesehen sind dies vor allem die Ersteller eines Dokuments oder von Dateien. Hier wurde definiert, wie die Loginformationen letztlich ins SIEM gelangen, was kritische Aktionen sein können und wie diese in den Loginfos erscheinen. Für Anwendungen, deren Loginformationen das SIEM nicht standardmäßig unterstützt, mussten zudem spezielle Parser geschrieben werden. Parser sind Scripte bzw. Filter, die diese Informationen quasi „durchlesen" und deren Inhalte für das SIEM aufbereiten. Nach dem parsen werden die Rohdaten sowie die geparsten Loginformationen veränderungssicher gespeichert und mit weiteren Informationen korreliert. Dazu dient die Korrelationsengine als integrierte Komponente der SIEM-Plattform. Sie führt automatisch und regelbasiert fortlaufende Analysen durch und protokolliert bzw. alarmiert alle beobachteten Aktivitäten. Dies schafft Echtzeit-Einblicke in Risiken oder kritische betriebliche Fehler, die sonst nicht möglich wären. Das Erstellen der Korrelationsregeln in einem SIEM-System läuft sehr individuell. Zum Teil werden Wizard-basierte Drag-and-Drop-Oberflächen zur Anpassung selbst hochkomplexer Regeln verwendet. Ein wesentlicher Punkt. Denn in diesem Projekt war und ist viel Bewegung in Bezug auf Sicherheitsrichtlinien an eine IT im Finanzwesen. Somit musste auch das Axians Team während der Umsetzung agil operieren.

Projektergebnis

Das SIEM der Bank ging erstmals im Sommer 2015 live. Just in time für eine EZB Prüfung. Mitte 2016 wurde die Installation ins neue Netz migriert und erweitert. Gleichzeitig starteten die Entwicklung der allgemeinen Betriebsprozesse in der IT-Sicherheit und die Neufassung der Dokumentation. Seit Anfang 2017 sind die Prozesse aktiv und seit Mitte 2017 auch die SIEM Dokumentation inkl. Fallvorlagen und den wichtigsten Quellen mit Anwendungsfällen angebunden. Die Bank erkennt und analysiert damit Angriffe oder Gefahren, die das Unternehmen, seine Netzwerke, Systeme, Applikationen und Services tagtäglich bedrohen – und kontert mit abgestimmten Maßnahmen, bevor Schaden entstehen kann. Durch die Prozesse ist der Weg vom Risiko bis zum Anwendungsfall klar definiert und sauber dokumentiert. Alle Anwendungsfälle werden zielgerichtet erstellt, umgesetzt und im Betrieb überwacht.

Axians bietet darüber hinaus auch die Verwaltung von SIEM-Lösungen nach Wahl. Unternehmen, die bereits ein SIEM-System für interne Sicherheitsanalysen einsetzen und Unterstützung bei der Administration und Wartung suchen, erfahren damit eine effektive Unterstützung durch versierte Cyber Threat-Analysten und Abwehr-Profis. Zudem gibt es die Option, ein lokales SIEM-System durch Axians verwalten und pflegen zu lassen – oder sein spezielles Security Information & Event Management komplett als „SIEM as a serivce" zu beziehen. In diesem Sinne: Carpe SIEM!

Quelle: Logrhythm

ANSPRECHPARTNER

Dirk Demuth (Sales, Axians) · E-Mail: info-itsecurity@axians.de · Tel.: +49 40 271661-0

axians.de

Stand 08/17