KUNDENREFERENZ

IS4IT KRITIS

Mehr Sicherheit bei OTTO dank Security Operations Center

DAS SOC DER IS4IT-GRUPPE IM PRAXISEINSATZ

Die Arbeit als Verantwortlicher für die Sicherheitsüberwachung in einem hochgradig digitalen Unternehmen ist bei den aktuellen Cyberbedrohungen nichts für schwache Nerven. Es gilt, sich auf die verschiedenen Bedrohungslagen vorzubereiten, um die Chancen für Angreifer auf ein Minimum zu reduzieren. Bei OTTO ist das Security Operations Center der IS4IT-Gruppe ein wichtiger Teil dieser Maßnahmen.

Für eine digitale Plattform wie OTTO ist eine funktionsfähige IT essenziell, da alle Prozesse von ihr abhängen. Informationssicherheit ist demzufolge eine der wichtigsten Grundlagen der Betriebsstabilität. Die Sicherheitsbedrohungen sind in digitalen Unternehmen jedoch sehr unterschiedlich. Ähnlich wie Einbrecher die Fenster eines Hauses als Zugang missbrauchen, kann jede Funktion der IT als Einfallstor für Hacker dienen. OTTO ist in der IT sehr breit aufgestellt und hat einen entsprechend heterogenen Schutzbedarf. Legacy- und Cloud-Anwendungen, die Campus-Infrastruktur, aber auch mobiles Arbeiten stellen das Security-Team vor die unterschiedlichsten Herausforderungen. Hinzu kommen gesetzliche Vorgaben zum Datenschutz und weitere neue Anforderungen und Richtlinien. So hat das BSI erst kürzlich Vorgaben für Anbieter digitaler Dienste erlassen. Das Ziel von OTTO ist es, auf derartige Veränderungen vorbereitet zu sein.

Robert Johns, Team Lead Security Monitoring bei OTTO, sieht Parallelen zur Feuerwehr. In der Brandbekämpfung weiß man: 100 %ige Sicherheit gibt es nicht, jederzeit kann etwas passieren und man trifft Vorbereitungen für eine etwaige Lage, um dann schnell und zielgerichtet handeln zu können. Für ihn gehört die Abwehr möglicher Bedrohungen zum Tagesgeschäft und mit der Zeit hat er gelernt, besonnen und zielgerichtet damit umzugehen.

Ob bei Bränden oder sicherheitsrelevanten Ereignissen: Als Verantwortlicher muss man sich auf die Einschätzungen von Fachleuten verlassen können und mit einem Team zusammenarbeiten, das kompetent und effizient agiert. Dank des IS4IT SOC-Teams ist Robert Johns sicher, immer rechtzeitig informiert zu werden, wenn potenzielle Sicherheitsbedrohungen adressiert werden müssen.

Das war nicht immer so. Die anfängliche Kooperation mit einem Anbieter führte immer wieder zu Schwierigkeiten bei der Priorisierung und Analyse von Sicherheitsevents. Als sich diese Probleme nach monatelangem Onboarding nicht legten und ein Sicherheitsvorfall die Defizite des Anbieters deutlich zeigte, machte man sich auf die Suche nach einem neuen Dienstleister. Auf Empfehlung und als Subkontraktor von IBM verantwortet das SOC-Team der IS4IT-Gruppe seit Januar 2022 die Überwachung der Systeme im Rahmen ihrer Managed Security Services.

> Die IS4IT-Gruppe hat mehr **Security-Dienstleistungen** im Portfolio, als wir aktuell benötigen. Damit weiß ich, dass mir im Ernstfall **weitere Service-Optionen** und Experten zur Verfügung stehen. So können wir unser Security-Team **bedarfsgerecht erweitern**. Das ist ein wichtiger Teil meines persönlichen **Sicherheitsempfindens**.
>
> *Robert Johns, Team Lead Security Monitoring*

ANFORDERUNGEN

- Aufbau des bestmöglichen Schutzes der geschäftskritischen IT-Infrastruktur
- Konzeption und Implementierung einer Sicherheitsarchitektur, die an zukünftige Bedrohungslagen anpassbar ist
- Optimale Vorbereitung auf verschiedene Bedrohungslagen zwecks Minimierung der Folgen von Cyberattacken
- Ständige Verfügbarkeit von erfahrenen Security-Analysten zur qualifizierten Bewertung von Sicherheitsvorfällen und Auffälligkeiten
- 24x7 Monitoring der gesamten sicherheitsrelevanten IT-Infrastruktur

LÖSUNGEN

- Security Consulting durch IS4IT Kritis
- IS4IT Managed Security Services
  - Managed SOC Service
  - Managed SIEM Service
- IBM-Lösungen

NUTZEN

- Kompetente Einschätzung der jeweiligen Bedrohungssituation durch Experten der IS4IT
- Sofortige Benachrichtigung in kritischen Situationen
- Wirtschaftliche Umsetzung durch Outsourcing
- Zugriff auf Erfahrungen aus anderen Unternehmen
- Verfügbarkeit von qualifizierten Ansprechpartnern für spezifische Fragestellungen
- Unterstützung beim Ausbau der Sicherheitsarchitektur

Rund um die Uhr werden im SOC der IS4IT-Gruppe alle sicherheitsrelevanten Meldungen geprüft und nach Bearbeitungsdringlichkeit priorisiert. Insbesondere abends, an Wochenenden und Feiertagen ist die qualifizierte Analyse wichtig, da bei unaufschiebbaren Events Mitarbeiter aus der Rufbereitschaft zur Problemlösung hinzugezogen werden.

Seit der Übernahme gab es keine gravierenden Vorfälle im Sinne harter Angriffe auf das Unternehmen. Unterschiedliche Angriffsversuche konnten nach sofortigem Alarm durch IS4IT vom OTTO-Team schnell unterbunden werden. Mithilfe des SOC wurden mögliche Probleme damit vor ihrer Entstehung behoben.

Zufrieden ist man bei OTTO auch darüber, dass man bei der Implementierung der SIEM-Infrastruktur mit QRadar für die Definition der Use Cases ausreichend Zeit investiert hat, sodass man jetzt nicht mit überflüssigen Alarmierungen belastet wird. Robert Johns empfiehlt: *„Hier sollte man von den Erfahrungen anderer SOC-Nutzer lernen. SIEM out of the box bietet ein Beispielregelwerk, das eine Basis darstellt. Nutzt man es 1:1 mit den zahllosen verfügbaren Logs seiner Systemlandschaft, kann es richtig viel Arbeit machen. Ich rate anderen Unternehmen daher, sich zusammen mit ihrem SOC-Partner die schützenswerten Themen herauszuarbeiten und die relevanten Use Cases zu definieren. Damit erspart man sich False-positive-Alarme, die sehr viel Bearbeitungsaufwand nach sich ziehen.“*

Der Aufbau eines eigenen 24x7 SOC-Teams ist für OTTO selbst nicht wirtschaftlich realisierbar. Neben dem Verzicht auf Synergieeffekte, die nur durch Erfahrungen in mehreren Unternehmen entstehen, müsste der Mitarbeiterstamm erheblich erweitert werden. Für einen klassischen Schichtbetrieb bei dem First-, Second- und Third-Level-Analyse durchgeführt werden, sind 13 bis 14 Mitarbeiter mit unterschiedlichen Kompetenzen notwendig. Dabei fallen für Level 3 keine ausreichenden Arbeitsmengen an, was zu Leerlauf führen würde – abgesehen davon, dass am Arbeitsmarkt keine Experten zu finden sind.

Auch wenn QRadar aus Sicht von OTTO eine betriebsstabile SIEM-Lösung darstellt, mit der man gut in der Lage ist, die Infrastruktur zu überwachen, ist SIEM im Security Monitoring nur ein Mittel zum Zweck. Mithilfe weiterer Tools sorgt man für die stetige Modernisierung der Überwachungsarchitektur – ob durch Vereinheitlichung der Arbeitsprozesse, automatische Reaktion oder Identifikation der Angreifer.

Zusammen mit IS4IT Kritis entwickelt OTTO die Konzepte zur IT-Sicherheit konsequent weiter, da man erkannt hat, dass man von den Erfahrungen des Cybersecurity-Experten erheblich profitieren kann. Aus Sicherheitsgründen will Robert Johns aber nicht über die Details sprechen – da behält er starke Nerven.

ÜBER DEN KUNDEN

Branche: **Handel**

Mitarbeiter: **6120**

OTTO steht heute für eine Handelsplattform, deren Umsatz 22/23 mit 6,3 Mrd. EUR die Bedeutung von Shopping im Internet verdeutlicht. Über 5000 Händler und Partner vermarkten rund 14,5 Millionen Produkte auf dem OTTO Marktplatz. Den erfolgreichen Produkthandel runden kundenorientierte Service-Angebote nahtlos ab.

Webseite: **www.otto.de/unternehmen**