KUNDENREFERENZ

IS4IT KRITIS

IS4IT Security Operations Center (SOC) überwacht IT-Infrastruktur

KERNKRAFTSICHERHEIT: NUR DAS BESTE IST GUT GENUG

Cyberangriffe im Bereich Kernenergie müssen um jeden Preis verhindert werden. Die Kritikalität der Anlagen macht absolute Sicherheit erforderlich, auch wenn diese aufgrund des Atomkraftausstiegs bereits stillgelegt sind oder sich im Rückbau befinden. Die regelmäßige Überprüfung der IT-Sicherheit gehört daher zum Standard jedes Anlagenbetreibers. Unabhängige Berater bewerteten im Rahmen einer 360-Grad-Analyse im Jahr 2018 die implementierten IT-Sicherheitsmaßnahmen des Unternehmens insgesamt positiv. Die wenigen bestehenden Verbesserungspotenziale wurden gemeinsam mit IS4IT konsequent realisiert.

Gutes noch besser machen

Kern der Optimierung war die Einführung eines umfassenden Security Monitorings, für das dem Unternehmen aber nicht nur die notwendige jahrelange Praxiserfahrung fehlte, sondern auch die eigenen Ressourcen. So sind bspw. für eine durchgängige Überwachung mindestens sechs Mitarbeiter nötig. Daher entschied sich das Management, das Security Monitoring an ein externes Security Operations Center (SOC) auszulagern.

Nach Evaluierung verschiedener Anbieter kam es zu einem Proof of Concept, in dem die ersten Anwendungsfälle durch das SOC-Team der IS4IT implementiert wurden. Nach acht Wochen waren Wirksamkeit und Mehrwert des IS4IT SOC belegt und die Vorarbeiten zur Umsetzung begannen mit dem Kick-off im Februar 2019.

Maximale Sicherheit von Anfang an

Die atomrechtlichen Verfahren sehen vor, sämtliche Prozesse gemäß Änderungsverfahren der Kategorie D abzuwickeln. Auch wenn dafür aufgrund der fehlenden nuklearsicherheitstechnischen Bedeutung keine Zusammenarbeit mit Behörden erforderlich war, stellten sie die IS4IT trotzdem vor besondere Herausforderungen.

Neben äußerst strikten SLA-Vorgaben musste das gesamte externe Team atomrechtlich überprüft werden. Darüber hinaus galt es nachzuweisen, dass das SOC den Kernkraftwerksbetrieb nicht negativ beeinflusst und dass es in allen Prozessen, in die IS4IT involviert wird, nicht zu Änderungsaktionen kommen kann, sondern ausschließlich lesender Zugriff erfolgt.

Keine besonderen Vorkommnisse

Nachdem sämtliche Voraussetzungen erfüllt waren, wurde das SOC im September 2020 mit dem Managed SIEM Service auf Basis von IBM QRadar erfolgreich in Betrieb genommen. Die Resultate bestätigen den hohen Grad der Abschirmung der Systeme.

> Bereits durch den **Proof of Concept** war offensichtlich, dass das Security Operations Center **effizient** ist und uns **echten Mehrwert** bietet. Die sinkende Anzahl der Incidents ist ein Beweis für die **Wirksamkeit der Sicherheitsmaßnahmen** – ein Ergebnis, welches im Bereich der Kernenergie selbstverständlich sein muss.
>
> *Energieversorger*

ANFORDERUNGEN

- Gewährleistung maximal möglicher Sicherheit
- Erfüllung sämtlicher Regularien des Atomgesetzes
- Nutzung des höchstmöglichen Grads an Expertise
- Entlastung des internen IT-Teams

LÖSUNGEN

- Managed Security Services von IS4IT Kritis / IS4IT
- Security Operations Center (SOC)
- Einführung und Konfiguration von IBM QRadar
- SIEM Service
- 24/7 Security Monitoring

NUTZEN

- Wirtschaftlichste Form der Umsetzung von Anforderungen
- Übergreifender Blick auf sämtliche sicherheitsrelevante Komponenten
- Korrelation scheinbar unabhängiger Events zur Identifikation von Gefahren
- Bereinigung der IT-Infrastruktur
- Skalierbare und sukzessiv erweiterbare Lösung

IS4IT überwacht nicht nur die gesamte Netzwerkinfrastruktur (Firewall, Netzwerkverkehr etc.) der Zonen Eins (Bürokommunikation) und Zwei (reaktornahe Systeme), auch sämtliche Events aus dem Bereich Endpoint Security (Active Directory, Virenschutz usw.) fließen in die Konsole ein, werden korreliert und im Zusammenhang beim Monitoring berücksichtigt. Aus verschiedensten Quellen gelangen so Daten in die SIEM-Applikation und ermöglichen, was sonst nicht möglich ist: einen ganzheitlichen Blick, durch den sich Anomalien erkennen lassen.

Im Rahmen der Analysen von Benutzer- und Netzwerkverhalten werden aktuell 40 verschiedene Szenarien adressiert. Außer der vielfältigen Überwachung der Benutzerkonten, der Kontrolle der Eingangsports sowie der Identifikation illegitimer Programme oder Services gehören auch ungewöhnliche Datenzugriffe oder unerlaubter Zugriff auf Netzwerkkomponenten zum Monitoring-Programm.

Trotz dieser umfassenden Kontrolldichte fallen nur zwei bis drei berichtsrelevante Tickets pro Monat an. Innerhalb der ersten zwölf Monate kam es zudem zu keiner kritischen Situation – aus Sicht des Kunden ein hervorragendes Ergebnis, da es belegt, wie gut die IT-Infrastruktur vor Cyberangriffen geschützt ist.

Zusatznutzen: Steigerung der Betriebsqualität

Als positiver Nebeneffekt der recht aufwändigen Sicherheitsanalyse trägt das SOC-Team dazu bei, die Qualität der IT-Infrastruktur zu verbessern.

Das liegt nicht nur daran, dass ein externer Blick auf die Systeme andere Facetten wahrnimmt, als es der internen IT möglich ist. Die Analyse der Daten aus den vielfältigen Quellen erlaubt es darüber hinaus, z. B. überflüssige Maschinen zu identifizieren oder aber auch Anomalien zu erkennen, die nicht sicherheitsrelevant sind.

So bemerkte das IS4IT-Team nächtlich wiederholt auftretenden ungewöhnlichen Traffic im WAN, das die drei Standorte des Energieversorgers vernetzt. Dank SIEM Service standen ausreichend Daten zur Verfügung, sodass die Experten der IS4IT die Ursache schnell lokalisieren konnten.

„Unser SOC hat seine Leistungsfähigkeit in einem Umfeld nachgewiesen, das kritischer nicht sein kann. Davon profitieren alle Kunden. Es sind die Shared Services, die das SOC so attraktiv machen“, fasst Manuel Noe, Geschäftsführer der IS4IT KRITIS GmbH, die Ergebnisse zusammen.

ÜBER DEN KUNDEN

Branche: **Energieversorger**

Mitarbeiter: **Rund 3 000**

Der Energieversorger aus dem Kernkraftbereich verfügt über fünf Reaktoren an drei Standorten. Der Rest befindet sich im Rückbau. Das Unternehmen setzt auf höchste Sicherheitsstandards. Daher erfolgt an dieser Stelle keine namentliche Erwähnung.

Stand: **März 2024**