Datenschutzhinweise
für Nutzerdaten bei der Verwendung von IT-Systemen

Aktuell betreibt die Brose IT-Security Abteilung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO ein zentrales Security Incident and Event Management (SIEM). Es handelt sich um eine Lösung, die Organisationen dabei unterstützt, Sicherheitsbedrohungen zu erkennen, zu analysieren und darauf zu reagieren, bevor sie den Geschäftsbetrieb beeinträchtigen.

Ziel ist es, das Unternehmen vor Sicherheitsrisiken in Bezug auf die IT-Systeme zu schützen. Cyberangriffe sowie unberechtigter Daten- und Informationsfluss müssen erkannt und verhindert werden. Mit Hilfe eines SIEMs können die wesentlichen Vorkommnisse transparent gemacht werden und dann individuell betrachtet und bearbeitet werden.

Das System erfüllt dabei die Rollen und Aufgaben, die auch im IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Baustein DER.1.A11 thematisiert und als notwendig für den Standardschutz erachtet und in bestimmten Bereichen auch zwingend gefordert werden. Darüber hinaus sind die entsprechenden Aufgaben und Funktionen ebenfalls ein erforderlicher Baustein (5.2.4) für die Erlangung einer TISAX-Zertifizierung in der bei Brose benötigten Ausprägung.

Das System klassifiziert selbständig Ereignisse vor und schlägt basierend auf Regelsätzen und bereits gewonnenen Erkenntnissen selbstständig Maßnahmen vor, wie auf die vorliegenden Ereignisse reagiert werden kann. Dies erleichtert die Bearbeitung der Sicherheitsvorfälle für das fachkundige Personal enorm und unterstützt dabei auch die vorher manuellen und dadurch fehleranfälligen Abläufe und Prozesse strukturiert und vollständig durchzuführen. Je nach Vorfall und Einstufung des Schweregrades kann das System auch vorab definierte Aktionen selbständig ausführen. Die eigentliche Bearbeitung von Vorfällen durch das Fachpersonal wird dadurch erheblich, einfacher und unanfälliger für Fehler. Dies trägt damit direkt zum günstigeren, sichereren und stabileren Betrieb der IT bei Brose bei.

Insbesondere folgende IT-Sicherheitsvorfälle sollen aufgedeckt werden:

- Missbräuchliche Verwendung von Brose-Resourcen, z.B. durch Installation eines Cryptominers, Nutzung als Dateiaustauschplattform oder zum Angriff weitere Ziele (intern und extern)
- Malwareangriff
- Phishingattacke
- Verschlüsselungs- oder Löschangriff (Ransomware/ Wiper)
- Nichtverfügbarkeit eines Services oder Benutzers (DoS/DDoS)
- Einschleusen fremder Hardware
- Accountmanipulation
- Kompromittierte Zugangsdaten
- Datenexfiltration
- Umgehung von Schutzmaßnahmen
- Ausweitung der Kompromittierung (Lateral Movement)
- Privilegienerweiterung
- Unbekannte Privilegierte Aktivität
- Abnormale Authentisierung & Zugriff
- Veränderung von Audit-Funktionen und Audit-Daten
- Zugriff auf geschützte Daten
- Abfluss geschützter Daten (Data Leakage)
- Zerstörung von Daten
- Physische Sicherheit (Manipulation/Diebstahl von Hardware)
- Missbrauch von Privilegien
- Einsatz gefährlicher, unerlaubter oder unerwünschter Software

Die verschiedenen SIEM-Produkte erhalten Daten aus unterschiedlichen lokalen Datenquellen über Standortkollektoren. Zu den lokalen Datenquellen zählen unter anderem Firewall Systeme, AntiVirus Lösungen und Systemprotokollierungen. Des Weiteren werden Daten aus Cloudanwendungen wie z. B. Microsoft M365, Azure, AWS etc. durch einen sogenannten Cloud Connector direkt von den SIEM-Systemen empfangen. Die Übertragung erfolgt in allen Fällen verschlüsselt.

Eine Speicherung der Daten erfolgt für maximal 180 Tage.

Neben zahlreichen technischen Daten werden insbesondere auch folgende personenbezogene Daten der Mitarbeiter verwendet:

- Name
- E-Mail
- IP Adresse
- Computeraccount-Stammdaten
- Berechtigungsgruppen
- Genutzte Dienste
- Kommunikationsranddaten (Gegenstellen, Dauer, Menge, Status, Parameter, angefragte Resourcen, …)
- IT-Nutzungsdaten (Userbezogene Logfiles wie An- und Abmeldedaten, Geo-Location der Systemverwendung, Useraktionen wie Dateizugriff)

Dies bedeutet, die Daten lassen Rückschlüsse auf die Aktivitäten der Mitarbeiter bei der Verwendung der IT-Infrastruktur zu. Dies gilt auch bei der privaten Nutzung der IT-Infrastruktur.

Ein Export von personenbezogenen Daten ist nicht vorgesehen und ist auch nur durch die Administratoren möglich. Die Nutzung der Informationen kann jedoch im Fall eines schweren Sicherheitsvorfalls durch andere Unternehmen erfolgen, die Brose hierbei als spezialisierte Dienstleister unterstützen. Mit diesen Unternehmen sind aber ebenfalls entsprechende vertragliche Regelungen in Form von Auftragsdatenverarbeitungsvertrag, Geheimhaltungsvereinbarung etc. abgeschlossen.
Eine Weitergabe der im SIEM gespeicherten Daten an Dritte ist nicht vorgesehen. Sollte es jedoch im Rahmen von Betriebsvereinbarungen gestattet sein, die Daten zur Aufdeckung von Straftaten zu verwenden, können Daten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO auch an Rechtsanwälte, Gerichte oder Strafverfolgungsbehörden weitergegeben werden.

Funktionsweise SIEM