Security Operations Center

Ein **Security Operations Center (SOC)** ist ein Zentrum, das Dienstleistungen für die IT-Sicherheit bietet: ein Verfahren zur Vorbeugung und Behandlung von unvorhergesehenen Schwierigkeiten. Die Aufgabe dieser Infrastruktur ist die Vorbeugung gegen das Risiko, das alle Aktivitäten der IT-Sicherheit mit Hilfe von Zentralisierung und Analyse aller menschlichen Ressourcen sowie der Hardware und Software zur Verwaltung des Sicherheitssystems beinhaltet. Dabei vereint es die drei Teilbereiche Menschen, Prozesse und Technologien um die Sicherheitslage einer Organisation zu steuern und zu verbessern.[1] Eine Struktur dieser Art wird 24 Stunden am Tag und für 365 Tage im Jahr von Personal, das die Performance der Plattformen sicherstellt und die Informationen analysiert und zusammenfasst, geschützt. Die operativen Verwaltungsprozesse, die das SOC steuern, sind vorhanden, um ständig das Restrisiko zu analysieren und bieten auch Schutz vor Einbruch durch vorübergehende Security Assessments. Da die Verwaltung von Netzwerk-Sicherheit eine Tätigkeit ist, die viel Zeit und Humanressourcen erfordert, ziehen es Unternehmen oft vor, den Dienst auszulagern bzw. an andere Unternehmen zu übertragen, die im Bereich der Informationssicherheit spezialisiert sind. Solch einem Partner die Verwaltung der Sicherheit des eigenen Firmennetzwerks anzuvertrauen, bewirkt eine erhebliche Kostensenkung und die Möglichkeit, die eigenen Kräfte auf das Kerngeschäft zu konzentrieren. Der Sicherheitspartner muss allerdings die Erbringung der Leistung von hoch qualifiziertem Sicherheitspersonal bereitstellen. Die Dienstleistung besteht aus dem kontinuierlichen Überwachen der Tätigkeiten der Firewall, IDS und der Antivirusprogramme, identifizieren kritischer Schwachstellen usw. Es handelt sich hierbei um sehr spezielle Arbeitsvorgänge, daher ist es erforderlich, dass die Mitarbeiter ständig auf neuestem Stand bleiben, um das Wissen über Technologien und die angewandten Methoden zu erhalten und zu vertiefen.

Inhaltsverzeichnis

Mögliche angebotene Dienstleistungen vom SOC

- Proaktive Analyse und Verwaltung der Systeme und Techniken der IT-Sicherheit
- Security-Device-Management

- Reporting
- Security-Alert
- DoS-Schadensbegrenzung
- Security-Assessment
- Technische Hilfe

Proaktive Analyse und Verwaltung der Systeme und Techniken der IT-Sicherheit

Dieser Dienst hat die proaktive Analyse der Systeme und Techniken der IT-Sicherheit an 24 Stunden pro Tag zum Ziel (IDS, IPS, Firewall etc.). Die Anti-Intrusions-Systeme ermöglichen die zentrale Verwaltung von Informations-sicherheits-Praktiken, damit potenzielle Angriffe aus dem Computer und dem Internet und Intranet identifiziert werden können. Das hierfür beauftragte Personal ist in der Regel sehr spezialisiert und qualifiziert, daher müssen z. B. Sicherheitsanalysten nur die Funktionen der Monitoring-Tools kennen statt die umfangreiche Gesamtausstattung der Sicherheitsvorkehrung. Die Skalierbarkeit der Hilfsmittel des SOC ist ein weiterer entscheidender Faktor; so ist es zum Beispiel relativ einfach möglich, ein neues IDS (Intrusion Detection System) zu den bereits bestehenden hinzuzufügen. Oft verwaltet das SOC auch einen Teil bezüglich des Policy-Managements, das z. B. die Rekonfigurierung der Sicherheits-Ausrüstung berücksichtigt. Die ursprüngliche Konfiguration der Geräte und die Sicherheits-Politik müssen ständig aktualisiert werden, indem die Entwicklung des Netzwerks des Kunden verfolgt werden.

Security-Device-Management

Das Security-Device-Management (SDM) entwickelt sich insbesondere um die zwei wichtigsten Prozesse:

- Fault-Management
- Configuration-Management.

Fault Management

Das Hauptziel des Fault Management ist, den optimalen und kontinuierlichen Betrieb der Sicherheitsinfrastruktur zu garantieren. Die Aktivitäten umfassen:

- die ständige Überwachung der Sicherheitsausrüstung des Kunden durch das SOC
- Erkennung und Alarm bei Faults (Aktivierung Trouble-Ticket)
- Ermittlung des entsprechenden Handelns zur Abhilfe
- Umsetzung der entsprechenden Maßnahmen zur Abhilfe
- die Restaurierung von Konfigurationen für den Fall ihrer Verluste nach einem Fault

Configuration-Management

Das Hauptziel des Configuration-Managements ist, die stetige Anpassung der Firewall-Strukturen an die Bedürfnisse des Kunden zu gewährleisten. Es deckt alle Geräte ab, die vom SOC verwaltet werden. Das Configuration-Management umfasst die Tätigkeiten der Konfigurierung und passt Policy-Filter oder Autorisierungen zum Fluss des Datenverkehrs von einer externen zu einer internen Quelle (oder umgekehrt) an, auf der Grundlage von:

- Adresse der Quelle
- Adresse der Bestimmungsstelle
- Netzwerk-Protokoll
- Service-Protokoll
- Protokollierung von Verkehrsdaten.

Reporting

Die Log von den Konsolen oder den eingesetzten Instrumenten werden normalerweise sorgfältig analysiert und wiederaufarbeitet, damit sie für den Kunden leicht verständlich gemacht werden. Dieses Reporting ist besonders wichtig, denn neben den Einzelheiten über eventuelle Eindringungsversuche von nicht berechtigten Einheiten oder über unvorhergesehene Schwierigkeiten, die im Reporting-Zeitraum sichtbar wurden, erlaubt es dem Kunden, Vorsorgemaßnahmen vornehmen zu können.

Security-Alert

Die Dienstleistung des Security-Alert wurde entwickelt, um den Kunden schnellstmöglich die Entdeckung neuer Sicherheitslücken mitzuteilen, um zeitnah die erforderlichen Gegenmaßnahmen zur Abschwächung oder Neutralisierung der Auswirkung der neuen Schwachstellen zu generieren.

DDoS-Schadensbegrenzung

Die DDoS-Schadensbegrenzung hat zum Ziel, die Folgen eines Angriffs der Art „Distributed Denial of Service“ zu mindern. Die Aufgabe dieser Dienstleistung ist, die korrekte Einleitung von erforderlichen Maßnahmen zum Schließen der Sicherheitslücke zu gewährleisten, wenn ein Kunde ein Alarmanzeichen erhalten hat. Die anzuwendenden Gegenmaßnahmen werden bewertet und ein „Reinigungs“prozess und eine evtl. Umleitung des Datenverkehrs werden in die Wege geleitet. Es erfolgt eine Meldung bei Ende der Attacke.

Security-Assessment

Einige Elemente, die normalerweise Bestandteil der Aktivitäten des Security-Managements sind, sind: das Vulnerability-Assessment und der Penetrationstest.

Das Vulnerability-Assessment ist entwickelt worden, um erkannte Schwachstellen der Systeme und auf ihnen installierten Services zu identifizieren. Eine solche Aktivität erfolgt mit Hilfe von spezifischen Technologien; sie werden für jedes Assessment einzeln konfiguriert, verbessert und personalisiert.

Der Penetrationstest wird durchgeführt, um bekannte oder noch unbekannte Schwachstellen des Systems, der Services und der Web-Anwendungen, die hierdrauf laufen, zu identifizieren. Der Vorgang des Penetrationstests ist in der Lage, auf sehr effektive Weise das Niveau einer bestimmten Sicherheitsbedrohung sowie die entsprechende Einschätzung der Auswirkung hervorzuheben. Eine solche Aktivität wird mit Hilfe einer großen Anzahl von Technologien, die für jede Bewertung konfiguriert, verbessert und personalisiert wird, aber auch auf manuelle Art und Weise für jeden Service, jedes System und jede Anwendung durchgeführt.

Technische Hilfe

Im Allgemeinen kann das SOC dem Kunden auch spezielle technische Unterstützung für alle Funktionsprobleme, Systemverletzungen, aber auch Neuerungen und Konfigurationen für Sicherheitshard- und software bieten. Die technische Hilfe zum Lösen der genannten Probleme kann aus der Entfernung oder vor Ort je nach Problemstellung und Vertragsausgestaltung zwischen den Vertragspartnern umgesetzt werden.

Siehe auch

- Informationssicherheit
- Sicherheitslücke
- Vulnerability Assessment und Schadensbegrenzung
- Buffer Overflow
- Exploit
- Firewall
- Antivirus

Einzelnachweise

1. Manfred Vielberth, Fabian Bohm, Ines Fichtinger, Gunther Pernul: *Security Operations Center: A Systematic Study and Open Challenges*. In: *IEEE Access*. Band 8, 2020, ISSN 2169-3536 (https://zdb-katalog.de/list.xhtml?t=iss%3D%222169-3536%22&key=cql), S. 227756–227779, doi:10.1109/ACCESS.2020.3045514 (https://doi.org/10.1109/ACCESS.2020.3045514) (ieee.org (https://ieeexplore.ieee.org/document/9296846/) [abgerufen am 5. Februar 2021]).