swisscom

Medienmitteilung

Cyber-Abwehr: Gefahr erkannt – gebannt

Swisscom weitet ihr Angebot an Managed Security Services aus und bietet ab sofort umfassende Threat Detection & Response-Lösungen für Unternehmenskunden an. So lassen sich Cyber-Gefahren frühzeitig erkennen und Unternehmen können sich umfassend schützen.

Die Bedrohungen für Firmen und Behörden durch Malware, Hacking oder Phishing ist Alltag. Swisscom als Netzbetreiber und umfassender Security-Spezialist entdeckt und blockiert monatlich Millionen Malware-Angriffe und 2'250 Phishing-Attacken. Waren früher die Attacken das Werk smarter, gelangweilter Jugendlicher, so stecken heutzutage professionelle Cyber-Kriminelle dahinter. Deren Angriffe haben eine neue Qualität und Quantität erreicht.

Wo kein Rauch ist, ist doch häufig Feuer

Mit dem Internet der Dinge, zunehmender künstlicher Intelligenz und Cloud-Anwendungen eröffnen sich den Cyberkriminellen ganz neue Möglichkeiten, Unternehmen zu schaden. So kapern Hacker sich vernetzte Alltagsgegenstände, bauen damit Bot-Netze auf und starten etwa DDoS-Attacken (Distributed Denial of Service). Die Angreifer kommen vermehrt auch auf leisen Sohlen, bleiben monate- bis jahrelang unbemerkt und richten enormen Schaden an. Das Perfide daran: Was man nicht sieht oder spürt, wird nicht bekämpft. Deshalb geht es darum, die Machenschaften von Cyber-Kriminellen frühzeitig zu erkennen (Detection) und professionell zu intervenieren (Response).

Bereit für die nächste Generation von Cyber-Attacken

Gegen diese Cyber-Bedrohung hilft nur eins: vorbeugen, frühzeitig erkennen und im Fall der Fälle mit Profis einschreiten. Dazu bietet Swisscom ihren Kunden ab sofort umfassende Threat Detection & Response-Lösungen an. Swisscom betreibt seit sieben Jahren ein 7x24-Stunden Security Operation Center für Unternehmenskunden in Zürich und hat ein eigenes Computer Security Incident Response Team (CSIRT). Die langjährige Expertise fliesst nun in die neue Threat Detection & Response-Lösung ein, die in vier modularen Service-Ausprägungen verfügbar ist:

1. Security Analytics as a Service
   Unternehmen erhalten via Security-Dashboard einen Überblick über potenzielle Sicherheitsvorfälle aus definierten Log-Daten. Der Kunde bezieht damit Security Analytics-Infrastruktur als Service. Die Analyse und Reaktion auf Sicherheitsvorfälle übernehmen die Unternehmen selbst.

2. Security Operation Center as a Service

   Ergänzend zu Security Analytics as a Service übernimmt Swisscom auch Security-Prozessleistungen. Erfahrene Security-Spezialisten analysieren im 7x24-Stunden-Betrieb potenzielle und bestätigte Sicherheitsvorfälle, interpretieren diese und geben Unternehmen konkrete Handlungsempfehlungen.

3. Computer Security Incident Response Team as a Service

   Zur Bewältigung von kritischen Sicherheitsvorfällen werden erfahrene Swisscom Security-Experten beigezogen. Diese leiten mit etablierten Tools und Prozessen den Security Incident Management Prozess ein und führen diesen durch.

4. Threat Intelligence as a Service

   Swisscom Experten informieren proaktiv über das Vorkommen von sensitiven Business- und Personeninformationen einer Unternehmung in öffentlichen und geschlossenen (z.B. Darknet) Netzen. Dadurch erhalten Kunden frühzeitig und einmalige Informationen, die auf mögliche Lecks im Unternehmen hinweisen.

Cyrill Peter, Head of Product Management Enterprise Network & Security bei Swisscom Enterprise Customers, sagt: "Bei den Angreifern stellen wir eine starke Professionalisierung und Industrialisierung fest. Dem können wir wie kein anderer entgegenwirken: Einerseits sehen wir durch unser Netz-Know-how sofort Anomalien und potenzielle Angriffe, andererseits fliesst das gewonnene Wissen aus Attacken automatisch in unsere Threat Detection & Response Services ein. Unsere Kunden profitieren damit von einer für die Schweiz einzigartigen Schwarmintelligenz".

Bern, 26. September 2017

Mehr zu Threat Detection & Response: https://www.swisscom.ch/detection