Telekom-Paket für Cyberresilienz

In Kooperation mit der Allianz schnürt die Telekom ein ab Sommer 2020 erhältliches IT-Sicherheitsgesamtpaket für Großunternehmen und Mittelstand ab einer Unternehmensgröße von 300 Mitarbeitern. Es besteht zunächst aus dem „Magenta Security Shield", einem vorkonfigurierten Blade-Server, den die Telekom ins Unternehmensnetz des Kunden einbindet und der die erforderlichen Sensoren sowie die nötige Software installiert. Hinzu kommen zentrale Security-Services aus der Telekom-Cloud – etwa Schwachstellenscans oder Schutz der Endpunkte – sowie die Integration in das Security-Operations-Center (SOC) des Konzerns. Dort beobachten über 240 Sicherheitsspezialisten die angeschlossenen Firmennetze und wehren Angriffe in Echtzeit ab. Allein 71 Millionen Angriffe verzeichnet die Telekom täglich auf ihren Honeypot-Systemen. Das neue Paket kostet samt Anbindung an das SOC eine monatliche Pauschale, die sich nach der Anzahl der Mitarbeiter pro Standort bemisst.

Im Sommer 2020 kommt eine weitere Schutzkomponente zum „Magenta Security Shield" hinzu: eine Cyberversicherung bei der Allianz Global Corporate & Specialty (AGCS) nach individueller Risikoanalyse beim Unternehmen. Die Konditionen sind laut Aussagen des Anbieters vorteilhaft, da das Risiko eines erfolgreichen Angriffs auf das Unternehmensnetz durch den Security Shield verringert ist.

Im Schadensfall springt die Versicherung bis zur vereinbarten Höhe ein und übernimmt auch die Kosten für den Ausfall und die Wiederherstellung von Daten oder Systemen sowie weitere Leistungen wie den Zugang zum IT-Forensik-Netzwerk des Versicherers oder Incident-Response-Services. Weitere Details sind online zu finden (ix.de/zwcq). (ur@ix.de)

Großangriff auf WordPress-Seiten

Das 30-Fache des normalen Volumens an Angriffsdaten auf WordPress-Seiten verzeichnete das Sicherheitsunternehmen Wordfence zwischen dem 28. April und dem 3. Mai. Ursache war eine groß angelegte Hackerkampagne, bei der die Kriminellen von 24 000 IP-Adressen aus versuchten, in mehr als 900 000 WordPress-Seiten einzubrechen. Dazu probierten sie, Cross-Site-Scripting-Schwachstellen (XSS) auszunutzen und auf den angegriffenen Seiten bösartigen JavaScript-Code zu platzieren, der die Besucher auf manipulierte Seiten umleiten sollte. Darüber hinaus scannte der bösartige Code nach Administrator-Log-ins, um dann automatisiert Backdoor-Konten zum Nachladen weiterer Schadfunktionen zu erstellen. Webfence mutmaßt, dass die Hacker zukünftig auf andere Schwachstellen ausweichen könnten, und nennt in seinem Blogbeitrag zum Angriff (siehe ix.de/zwcq) die Indicators of Compromise (IoCs), anhand derer Webseitenbetreiber feststellen können, ob ihre Seite kompromittiert wurde. Dazu gehören beispielsweise spezielle Zeichenfolgen in der Nutzlast oder auch Zeitstempel, die angeben, wann die Seite das letzte Mal auf eine erneute Infektion geprüft wurde, und die in der Datei debugs.log mit falscher Schreibweise gespeichert sind.

Die Mehrheit der beobachteten Angriffe zielt auf Schwachstellen, die seit Monaten und Jahren bekannt sind und gepatcht wurden. Daher ist die beste Prävention – eine Binsenweisheit in der IT-Sicherheit –, alle Plug-ins auf dem neuesten Stand zu halten und sämtliche Plug-ins, die aus dem WordPress-Plug-in-Repository entfernt wurden, zu deaktivieren und zu löschen. Weitere Details zu den Angriffen zeigt der vollständige Blogbeitrag.

(ur@ix.de)

Kurz notiert

Wie so viele andere Veranstaltungen finden auch die traditionell im Sommer in Las Vegas abgehaltenen großen **Hackerkonferenzen Black Hat und DEF CON** in diesem Jahr online statt.

Kriminelle mit Skrupeln: Während viele kriminelle Gruppierungen auch währen der Corona-Pandemie gezielt Krankenhäuser und andere medizinische Einrichtungen angreifen, um hohe Lösegelder zu erpressen, haben die Hintermänner der Ransomware Shade/Troldesh sich nicht nur bei ihren Opfern entschuldigt, sondern mehr als 750 000 Entschlüsselungs-Keys und eine selbst geschriebene Decryption-Software veröffentlicht.

Die Videoaufzeichnung der **Onlinekonferenz „Best of IT-Security"** ist für 199 Euro im heise shop als beliebig oft abrufbarer Stream erhältlich. Die von *iX* und c't ausgewählten Vorträge behandeln in 10 Stunden Themen wie Emotet bekämpfen, Post-Quanten-Kryptografie (mit Comics erklärt), Sicherheitskonzepte für KMU und vieles mehr. Security-Interessierte finden im Shop auch zahlreiche Webinare, etwa mit Bruce Schneier oder zur Absicherung von Windows 10 – live oder im Nachgang (alle Informationen unter ix.de/zwcq).

Videokonferenzsysteme sicher betreiben

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Mitte April sein „Kompendium Videokonferenzsysteme" veröffentlicht. Das rund 170 Seiten starke Werk (zu finden über ix.de/zwcq) soll Beschaffern, Betreibern, Administratoren und anderen dabei helfen, den gesamten Lebenszyklus organisationsinterner Videokonferenzsysteme sicher zu gestalten. Das Kompendium vermittelt Fakten und Ratschläge für alle Phasen, von der Planung über die Beschaffung und den Betrieb bis hin zum Aussortieren der Software.

Das Dokument orientiert sich an der IT-Grundschutzsystematik und beschreibt neben dem technischen Aufbau solcher Systeme und den typischen Gefährdungsszenarien die Basis- und Standardanforderungen sowie Anforderungen für erhöhten Schutzbedarf. Wie Videokonferenztechnik in behördlichen Bereichen mit Geheimhaltungsgrad VS-NfD (Verschlusssache, nur für den Dienstgebrauch) eingesetzt werden darf, soll eine noch in Arbeit befindliche Publikation regeln. Neben Maßnahmen zur Absicherung und Beispielen für die Raumausstattung finden sich auch Hinweise zu den speziellen Herausforderungen, die mit Cloud- und KI-Diensten einhergehen. (ur@ix.de)

Mehr Datenpannen im vergangenen Jahr

Aus den Jahresberichten einiger Landesdatenschutzbehörden lässt sich eine Zunahme von Datenpannen ablesen. In Bayern gab es 2019 nach Aussage der dortigen Datenschutzbehörde an manchen Tagen bis zu 20 Meldungen über Datenpannen, in Berlin im gesamten Jahr über 1000 Meldungen. In Bremen verdoppelte sich die Zahl im Vergleich zum Vorjahr auf über 80.

Grundsätzlich ist es für Unternehmen mit Datenpannen günstiger, diese von sich aus bei der Behörde zu melden. Erfährt die Behörde von Betroffenen und nicht vom verantwortlichen Unternehmen davon, drohen empfindliche Bußgelder nach der Datenschutz-Grundverordnung. Um die Unsicherheiten bei Unternehmen, aber auch Datenschutzbehörden darüber zu beseitigen, was im Detail als meldepflichtige Datenpanne anzusehen ist, beschäftigt sich nun ein Arbeitskreis der Datenschutzkonferenz mit dieser entscheidenden Frage.

Tobias Haar (ur@ix.de)