

Aktuelles

TTD (time to detect) - Die neue Zeitrechnung

22.10.2018



Weltweit gibt es heute wahrscheinlich mehr Hacker und Cyber-Kriminelle als Unternehmen. Die entscheidende Frage lautet daher ist nicht „ob“ und „wann“ sich ein Unternehmen im Fokus krimineller Aktivitäten befindet, sondern aus welchen Gründen und mit welchen Mitteln Eindringlinge versuchen an Daten und Firmengeheimnisse zu kommen.

Cyberkriminalität ist einer der schnellst wachsenden Wirtschaftszweige mit professionellen Strukturen – fest in den Händen ausländischer Geheimdienste und der organisierten Kriminalität. Im Kampf gegen diese hochgerüsteten Wirtschaftsspione bieten klassische Verteidigungssysteme kaum noch Schutz. Wer hier nicht untergehen möchte, muss sich permanent neu erfinden. Neue Strategien und Verteidigungssysteme sind daher kein Selbstzweck, sondern das Ergebnis einer sich stetig verändernden Sicherheitsbedrohung.

Zu den wichtigsten Erkenntnissen der letzten Jahre gehört die Tatsache, dass bestimmte Malware-Varianten die Unternehmensgrenzen mühelos passieren. Angriffe dieser Kategorie sind in der Regel „unsichtbar“ und „lautlos“ und sie werden meistens erst im Nachhinein anhand ihrer Auswirkungen entdeckt. Und dabei spielt der Faktor Zeit die entscheidende Rolle. Während voneinander autark agierende Einzelsysteme (meist von verschiedenen Herstellern) den Angriff oftmals erst nach Wochen bemerken, verfügt Cisco über ein Set an kollaborierenden Systemen, die Anomalien meistens innerhalb von Stunden enttarnen.

Dieser immense Zeitgewinn hilft den betroffenen Unternehmen den potentiellen Schaden zu minimieren. Denn einige aggressive Malware-Varianten lassen sich erst durch das Einspielen von Backups vollständig beseitigen. Je nachdem wie weit zurückgesichert werden muss, kann dies für die angegriffenen Unternehmen existenzbedrohend sein.

Stemmer unterstützt seine Kunden bei der Planung und Umsetzung einer ganzheitlichen Security-Strategie. Als zertifizierter Cisco Security Master verfügt Stemmer über mehrere Security Teams mit hochqualifizierten Consultants und Engineers. Unter dem Motto „Hybrid Everything“ kombinieren wir Private Cloud, Public Cloud und On Premise Bausteine zu flexiblen, effizienten und sicheren Infrastruktur-Lösungen. Dabei kann Security niemals isoliert betrachtet werden - sie ist immer ein wesentlicher Bestandteil aller Lösungen.

Stemmer GmbH
Peter-Henlein-Straße 2
82140 Olching

Telefon: +49 (0)8142 45 86-0
Telefax: +49 (0)8142 45 86-199

E-Mail: info@stemmer.de
Internet: www.stemmer.de

