Interview mit Stefan Strobel, Cirosec, auf der IT-Defense

IT-Sicherheit braucht Risiko-Management

geschrieben von LANline/Dr. Wilhelm Greiner am 26.02.2014

Am Rande der von Cirosec veranstalteten und stets hochkarätig besetzten Security-Konferenz IT-Defense (LANline berichtete), die dieses Jahr in Köln stattfand, sprach LANline mit Stefan Strobel, dem geschäftsführenden Gesellschafter und Gründer von Cirosec, über aktuelle Trends und Probleme im IT-Security-Markt. Die Themen reichten vom NSA-Skandal über Malware-Abwehr bis zu Bring Your Own Device (BYOD).

LANline: Herr Strobel, wie wirkt sich der von Marcus Ranum in dessen Keynote kritisierte NSA-Skandal auf Ihr Security-Beratungsgeschäft aus?

Strobel: Für Großunternehmen spielt das keine große Rolle. Diese Unternehmen haben eigene Security-Abteilungen, denen die Verhältnisse längst klar waren. Für sie waren die NSA-Vorgänge also keine Überraschung. Den KMU-Markt hingegen haben diese Ereignisse aufgeweckt. Hier waren Edward Snowdens Enthüllungen eine hilfreiche Awareness-Kampagne - deren Wirkung aber schon wieder abflaut.

LANline: Wie sollte ein Mittelständler nun reagieren?

Strobel: Ein Unternehmen muss wissen, was seine Kronjuwelen sind, um sich dann zu fragen: Was ist mir deren Sicherheit wert? Daraus leitet sich ein Budget und letztlich ein Bündel zu ergreifender Maßnahmen ab. Erforderlich ist also ein Risiko-Management.

LANline: Wie gut ist denn der Mittelstand in Sachen Risiko-Management?

Strobel: Im Mittelstand freut man sich häufig schon, wenn es einen Sicherheitsbeauftragten gibt. Oft ist das Sicherheitsdenken hier rein reaktiv und von Trends getragen. So diskutiert man heute viel über Apple-IOS- und Android-Sicherheit, aber kaum ein KMU hat so wichtige Sicherheitsbausteine wie NAC (Network Access Control, d.Red.) oder WAF (Web Application Firewall, d.Red.) im Einsatz.

LANline: Wie kommt das?

Strobel: Die Kernfrage muss sein: Was motiviert mich zu Investitionen in IT-Sicherheit? Hier mangelt es oft an Überblick über die Bedrohungsszenarien und einer Impact-Analyse. Stattdessen stürzt man sich - und da ist die IT-Presse nicht ganz unschuldig - auf neue Produkte und APTs (Advanced Persistent Threats, d.Red.). Doch hat Threat Defense mittels Lösungen wie Fireeye tatsächlich eine so hohe Priorität? Zumal fortschrittliche Malware inzwischen oft schon erkennt, dass sie in Systemen wie Fireeye läuft, und sich dann unauffällig verhält. Doch die Entscheidungen treffen nicht die IT-Experten, sondern die Führungskräfte, und diese sind oft eher emotional getrieben.

LANline: Auch um die Themen NAC und WAF gab es damals in der Fachpresse jeweils einen kleinen Hype - oder, wenn Sie so wollen, ein Hypelet. Warum konnten sich diese beiden Lösungsansätze bisher nicht flächendeckend durchsetzen?

Strobel: Im Fall einer WAF ist die interne Überzeugungsarbeit schwierig. WAF kostet Energie, man fürchtet einen hohen Aufwand bei der Einrichtung einer WAF, und jede Änderung an einer Web-Applikation muss man an der WAF nachziehen. So etwas wie Fireeye hingegen kostet auf den ersten Blick „nur Geld“. Bezüglich NAC wiederum haben viele Unternehmen jahrelang abgewartet, wie Cisco und Microsoft vorgehen werden. Und an dieses Warten hat man sich dann offenbar gewöhnt.

LANline: Was sind denn aktuelle Hype-Themen, mit denen sich Security-Verantwortliche tatsächlich befassen sollten?

Strobel: Hier fallen mir vor allem die Mikrovirtualisierung von Bromium und die Desktop-Virtualisierung ein, wie sie Moka5 betreibt. Bromiums Microvisor virtualisiert nicht vertrauenswürdige Prozesse innerhalb von Windows oder auch Mac OS X, er kapselt zum Beispiel jede Browser-Session. Diese Mikrovirtualisierung arbeitet nicht pro System-Call wie frühere - und immer umgehbare - Sandboxing-Techiken, sondern nutzt die Hardwarevirtualisierung von Intel VT-x. Deshalb kommt Bromium auch mit nur 10.000 Zeilen Code aus. Moka5 wiederum virtualisiert Endgeräte ähnlich wie VMware Workstation, es gibt sie aber auch für Smartphones und Tablets. So kann man zum Beispiel für BYOD virtualisierte Clients betreiben, die aber zentral verwaltet werden. Die Moka5-Architektur nutzt dabei ein Layer-Management: Die Aktualisierung eines Layers bedingt nicht automatisch Upgrades der übrigen Schichten.

LANline: Stichwort BYOD: Sind deutsche Unternehmen, die BYOD aktiv angehen, Einzelfälle oder entsteht hier tatsächlich ein Trend?

Strobel: Die Unternehmen, mit denen wir sprechen, bevorzugen eher CYOD (Choose Your Own Device, der Arbeitgeber bietet eine Auswahl an modernen Endgeräten, d.Red.). Das ist sicherer als die geschäftliche Nutzung von Privatgeräten, da das Unternehmen entscheiden kann, was auf das Gerät aufgespielt werden darf. BYOD birgt zudem Risiken wie die Verwendung veralteter Android-Geräte. In vielerlei Hinsicht ist BYOD heutzutage allerdings kein IT-Sicherheitsproblem mehr, sondern eher ein organisatorisches und juristisches Problem. Denn aus Security-Sicht ist mit Apples IOS 7 ein Sicherheitslevel erreicht, mit dem man gut leben kann, wenn das Unternehmen die Nutzung der Endgeräte mit einer Mobile-Device-Management-Lösung reglementiert. Die Frage ist hier also eher, wie komplex durch BYOD die Betriebsvereinbarungen werden.

LANline: Wird sich BYOD oder CYOD langfristig durchsetzen?

Strobel: Unsere Kunden bevorzugen, wie gesagt, derzeit eher CYOD. Allerdings hat im IT-Markt bekanntlich nichts Bestand. Ein IT-Entscheider muss ja heute oft schon froh sein, wenn er die letzten zwölf Monate nicht falschgelegen hat.

LANline: Herr Strobel, vielen Dank für das Gespräch.