Interview mit Cirosec-Geschäftsführer Stefan Strobel

Mit Bordmitteln gegen Ransomware

20. Februar 2020 | Von Dr. Wilhelm Greiner.

Schlagwörter: Cirosec, Malware, Mikrosegmentierung, Ransomware, Security Awareness, Security-Management, Segmentierung, Windows-Sicherheit

Im Nachfeld der Cirosec-Sicherheitskonferenz IT-Defense, die dieses Jahr in Bonn stattfand, sprach LANline mit Cirosec-Geschäftsführer Stefan Strobel über die Analyse der Bedrohungslage, die Abwehr von Ransomware-Angriffen, Windows-Sicherheit, Application Whitelisting und die Bedeutung effektiver Security-Awareness-Arbeit.

LANline: Herr Strobel, derzeit geht in den Unternehmen die Angst vor Erpressersoftware (Ransomware) um. Wie ermittelt Cirosec in Kundenprojekten die Anfälligkeit eines Unternehmens für Malware wie zum Beispiel Ransomware?

Stefan Strobel: In unseren Beratungsprojekten stellen wir das Malware-Schutzkonzept des Kunden anhand einer Wirksamkeitsmatrix auf den Prüfstand. Unsere Matrix gliedert die möglichen Malware-Probleme in eine Vielzahl von Zeilen, die Abwehrmechanismen des Kunden wiederum sind in den Spalten abgebildet. So lässt sich detailliert veranschaulichen, wo Lücken in der Abwehr bestehen. Auf dieser Basis können wir dann genau aufzeigen, wie man mit möglichst geringem Budget den größten Effekt erreichen kann.

LANline: Als Hilfsmittel gegen Ransomware wird immer wieder zu Backups geraten. Aber dann ist das Kind ja schon in den Brunnen gefallen. Zu welchen Maßnahmen jenseits von Backups raten Sie für die Abwehr von Ransomware?

Rät zur Nutzung der kostenlosen Windows-Bordmittel, um sich besser gegen Ransomware zu rüsten: Stefan Strobel, Geschäftsführer des Security-Beratungshauses Cirosec. Bild: Cirosec

Stefan Strobel: Backups sind natürlich ein wichtiges Mittel, um Ransomware-Angriffe mit geringem Schaden zu überstehen. Aber oberste Priorität sollte es eigentlich sein, solche Vorfälle von vornherein zu verhindern. Eine grundlegend wichtige, aber leider oft vernachlässigte Maßnahme ist es hier, den Endanwendern die lokalen Administratorrechte zu entziehen. Auf unserer Security-Konferenz IT-Defense 2020 in Bonn hat Sami Laiho, einer der weltweit bekanntesten Experten für Windows-Sicherheit, kürzlich anschaulich herausgearbeitet: Wenn man die meist kostenlosen Security-Funktionen von Windows 10 – AppLocker, Windows Defender ExploitGuard, Windows Defender CredentialGuard usw. – zum Einsatz bringt, dann ist man gegen Ransomware-Angriffe gleich viel besser gerüstet.

LANline: Stichwort AppLocker: Seit Jahren hört man von unterschiedlichen Seiten, Application Whitelisting sei zu aufwendig und deshalb nicht praktikabel. Was macht Microsoft mit AppLocker besser?

Stefan Strobel: Application Whitelisting galt lange als sehr komplex, aber inzwischen hat man gelernt, dass man das Thema anders angehen muss: Statt gänzlich auf Application Whitelisting zu vertrauen, sollte das Verfahren als Hilfmittel dienen, um erst einmal eine Basissicherheit von 90 Prozent zu erreichen. Zum Beispiel lassen sich mit AppLocker Zugriffe auf Verzeichnisse begrenzen, in denen die Programme tatsächlich stehen sollen – Malware landet erst einmal im temp-Verzeichnis, es ist also sinnvoll, dieses auszunehmen. Zugleich lässt sich der Zugriff damit auf Verzeichnisse begrenzen, die für die Endanwender schreibgeschützt sind. Allein diese Maßnahme erhöht den Aufwand für Angreifer schon enorm. Ergänzend können Unternehmen auf ihren Firewalls oder Security-Gateways jene Content-Typen blockieren, die für das Gros der Endanwender nicht erforderlich sind, also zum Beispiel PowerShell-Skripte. Auch Makros lassen sich gleich auf den Gateways automatisiert aus Office-Dokumenten entfernen. So erzielt man mit wenigen pragmatischen Maßnahmen bereits ein deutlich höheres Sicherheitsniveau.

LANline: Welche ergänzenden Maßnahmen zur Endpoint-Absicherung sind auf Netzwerkebene angeraten?

Stefan Strobel: Je nach Kontext sollte man mit Netzwerksegmentierung arbeiten, also zum Beispiel Controlling, SAP oder Produktion vom restlichen Netzwerk trennen. Oder man nutzt gleich eine Mikrosegmentierung: Firewalls auf allen Endgeräten erlauben dann die Kommunikation nur in dem Umfang, der tatsächlich erforderlich ist.

LANline: Wie muss man sich eine solche Mikrosegmentierung genau vorstellen?

Stefan Strobel: Die Adaptive Security Platform von Illumio zum Beispiel ermöglicht eine automatische intelligente Limitierung von Kommunikationsbeziehungen. Illumios Software protokolliert, wer mit wem über welche Ports spricht, erstellt eine App Dependency Map und korreliert diese mit der Asset-Datenbank. Auf Knopfdruck kann der Administrator dann die Windows-Firewalls der Endpunkte und die Linux-iptables der Server mit den passenden Regelwerken bestücken.

LANline: Welche Rolle spielt dabei die Security Awareness – und wie lässt es sich vermeiden, dass die Endanwender durch den Fokus auf eigenverantwortliches Handeln den Schwarzen Peter für Mängel der Sicherheitsstrategie zugeschoben bekommen?

Stefan Strobel: Wie Lance Spitzner, der Leiter des Security-Awareness-Programms beim SANS Institute, in seiner Keynote auf der IT-Defense betont hat: Die IT darf nicht immer nur auf die Endanwender zeigen, sondern muss sich an die eigene Nase fassen. Denn Security-Fachleute

leben oft in einer ganz anderen Welt. Deshalb erstellen sie mitunter Vorschriften, die für den Laien nicht verständlich sind. Das Security-Team sollte vielmehr mit der Frage nach dem Warum anfangen, um die Endanwender zu mehr Achtsamkeit zu motivieren. Spitzners Rat an die IT-Teams war deshalb: Sprecht mit den Kommunikationsspezialisten aus eurem Marketing und holt sie mit ins Boot!

LANline: Herr Strobel, vielen Dank für das Gespräch.

Dr. Wilhelm Greiner ist freier Mitarbeiter der LANline.