Schwachstelle Endgerät

Stefan Strobel, Geschäftsführer des IT-Beratungsunternehmens Cirosec, über Bedrohungen und Präventionsmöglichkeiten auf dem IT-Sektor.

Ein Großteil der 490 Aussteller auf der it-sa hat IT-Sicherheitsprodukte und -lösungen angeboten. Wie kann man herausfinden, welche Produkte geeignet sind?

Strobel: Man muss sich zunächst darüber klar werden, was man schützen will und wo die Schwachstellen im eigenen System liegen. Dann muss man sich einen Überblick verschaffen, welche Bedrohungen relevant sind – wobei diese einem beständigen Wandel unterliegen. Weiters muss man sich im Klaren sein, dass eine bloße Implementierung von Programmen allein nicht ausreicht. Deren Anwendung muss verstanden werden. Es genügt nicht, wenn Alarme einfach weggeklickt werden. Zudem müssen organisatorische Maßnahmen getroffen werden.

Reicht es, eine Firewall und ein Antiviren-Schutzprogramm zu installieren?

Strobel: Heutzutage nicht mehr, zumindest nicht als alleinige Maßnahme. Es gibt Möglichkeiten, Firewalls zu umgehen. Der klassische Virenschutz hat heute nur noch eine Erfolgsrate von weniger als 50 Prozent. Manche Experten meinen sogar, dass diese eher bei 30 Prozent liegt. Das liegt unter anderem daran, dass Malware sich so rasch ändert, dass sie früher beim Opfer ankommt, als Antiviren-Signaturen verfügbar sind. Ferner werden gezielte, auf ein bestimmtes Unternehmen zugeschnittene Angriffe nicht erkannt. Phishing-Mails sind mittlerweile so perfekt gestaltet, dass sie kaum mehr als solche erkannt werden. Die Bandbreite von dDoS-Angriffen reicht mittlerweile fast schon in den Terabit/sec-Bereich. Es gibt Firmen, die erkannte Schwachstellen verkaufen, oder Tools, mit denen Schadprogramme mit wenig Wissen hergestellt und in Umlauf gesetzt werden können. Die Erkennung nach alten Mustern hinkt den Angriffen immer hinterher.

IT-Experte Stefan Strobel (Cirosec): „Bei Endgeräten besteht noch großes Potenzial für Prävention."

Kann man serverseitig Schutzmaßnahmen treffen, sodass Schadprogramme gar nicht bis zum Endgerät durchkommen?

Strobel: Angesichts der Umgehungsmöglichkeiten funktioniert das in der Praxis leider nicht. Die Angriffe richten sich gegen das schwächste Glied in der Kette, und das ist das Endgerät. Bei diesem muss der Hebel angesetzt werden.

Welche neueren Techniken bieten sich an?

Strobel: Eine Möglichkeit ist, Programme, die ausführbare Dateien enthalten, zunächst in einer abgesicherten Umgebung zu beobachten, wie sie sich weiterentwickeln. Nach diesem Prinzip arbeiten Sandbox-Verfahren. Das kann allerdings bis zu einigen Minuten dauern. Man kann aber auch einem Angreifer, der auf der Suche nach Schwachstellen ist, eine solche als Falle anbieten und dann nachforschen, ob der Suchende auf Grund entsprechender Ermittlungen bereits als Angreifer bekannt ist. Typische Muster für einen gezielten Angriff, sogenannte Indicators of Compromise, bestehen darin, dass versucht wird, intern Rechte zu erweitern. Durch Analyse solcher Vorgänge können Einbrüche erkannt und beispielsweise zum Anlass genommen werden, Passwörter zu ändern. Bei Industrienetzen, bei denen sich im Produktionsbetrieb vergleichsweise wenig ändert, fallen Anomalien leichter auf und haben einen Alarm sowie Abwehrmaßnahmen nach sich zu ziehen. Für Personalabteilungen von Unternehmen oder Versicherungen, die eine Vielzahl von Anhängen zu E-Mails erhalten, wie Bewerbungen Fotos, Dokumente, sind Verfahren interessant, die einlangende Anhänge zerlegen und neu zusammensetzen. Malware wird dadurch neutralisiert.

Wie funktionieren neuartige Antiviren-Programme?

Strobel: Antiviren-Programme der nächsten Generation setzen neuronale Netzwerke und maschinelles Lernen ein, um Angriffe zu erkennen und abzuwehren. Es gibt auch Firmen, die erkannte Indicators of Compromise aufkaufen und den Internetverkehr ihrer Kunden anhand solcher Auflistungen überprüfen. Letztlich gibt es auch die Lösung, die zu schützenden Rechner vom Internet physisch zu trennen, wozu man allerdings zwei Browser braucht. Bei allem ist aber zu bedenken, dass sich Informationssicherheit kontinuierlich anpassen muss, sowohl von der Informationstechnik als auch von der Bedrohungslage her. Dazu kommen die legistischen Änderungen. Gerade bei Endgeräten besteht noch großes Potenzial für Prävention.

Interview: Kurt Hickisch

FOTO: KURT HICKISCH