Schutz aus dem Netz?

Das Internet wird immer wichtiger für die Sicherheit

Stephan Mayer

Bis jetzt echauffierten sich Experten bei Sicherheitslücken in Webcams, Rollladensteuerungen und derlei mehr vor allem über die angeblich fahrlässigen Hersteller, die ihre Produkte nicht sicher genug machen – natürlich aus reiner Profitgier und Gedankenlosigkeit. Und man echauffierte sich noch mehr über die Gemeinheit, dass diese Hersteller selbst dann diese Schwachstellen nicht beseitigten, wenn sie von ihnen wussten. Statt aber auf die Hersteller von IoT-Geräten zu schimpfen, die die Sicherheit ihrer Produkte sträflich vernachlässigen würden, sollten lieber effektive Schutzstrategien im Netz entwickelt werden, die mögliche Schwachstellen gar nicht erst zum Tragen kommen lassen.

Stephan Mayer ist freier Fachjournalist in Hösbach

Eigentlich ist die ganze Aufregung um die Sicherheitslücken ein Sturm im Wasserglas, sieht man sich die technische Struktur der betroffenen Geräte an. Gerade im privaten Umfeld sind dies Gadgets, deren Onlinenutzwert meist eher zweifelhaft ist, im unternehmerischen Umfeld hingegen sind es meist Steuerungen für Maschinen oder aber Anwesenheits- und Zutrittskontrollsysteme – beide von großer Wichtigkeit für Unternehmen. Doch die implementierte „Intelligenz" muss zumeist mit sehr wenig Rechenleistung und Speicher auskommen. Dies bedeutet letztlich, dass es nur bedingt, wenn überhaupt möglich ist, Sicherheitsfunktionen mit einzubauen, ohne die Grundfunktionalität zu stören.

Das Netz wird wichtiger

Insofern wird das Netz, über das diese Geräte funktionieren, immer wichtiger für die Sicherheit von Unternehmen und für Privathaushalte. Wenn die Geräte sich nicht selbst schützen können, dann muss dies eben das Netz für sie erledigen. Konzepte hierfür existieren schon seit fast zehn Jahren, doch erst heute werden die von IT-Lehrstühlen entworfenen Szenarien tatsächlich ernst genommen.
Zunächst musste einfach der Blick für die mögliche Bedrohung geschärft werden – dies wird meist durch einen großangelegten Angriff mit schlagzeilenträchtigen Auswirkungen erreicht. Denn der zeigt nicht nur die Gefährdung, sondern auch, dass die Bedrohung real ist und dass man gegen sie etwas unternehmen muss. Dabei ist Abhilfe leichter gesagt als getan. Gerade Produkte, die derzeit für den IoT-Markt entwickelt werden, besitzen sehr kurze Lebenszyklen – das Nachfolgeprodukt kommt erheblich schneller auf den Markt als Softwarekorrekturen für nicht mehr verkaufte Produkte programmiert werden können.
Hinzu kommt: Das Internet der Dinge (Internet of Things – IoT) steht erst am Anfang. Dazu zählen z.B. die intelligenten Stromzähler. Sie gestatten zwar den Zugriff auf den Zählerstand durch das Versorgungsunternehmen, verfügen aber sonst über keine weiteren Funktionen: Hinweise auf Verbrauchsspitzen, auf Leerverbrauch durch defekte Geräte o.ä. – Fehlanzeige. Aber: Jede derartige Funktion könnte – wenn sie denn von außen ablesbar ist – auch vom Energieversorger abgerufen werden, oder vom geharnischten Nachbarn oder von einem Einbrecher im Auto zwei Straßen weiter.
Diese Offenlegung eigentlich privater Daten gilt dann aber auch für nahezu jedes andere smarte Gerät: Eine Smart Watch, deren Betriebssystem eine Schwachstelle aufweist, macht gesundheitliche Probleme publik oder verrät sie gleich an die Krankenkasse. Oder der intelligente Türöffner mit Kamera könnte auch vom Nachbarn ebenfalls abgerufen werden, falls der ein ähnliches Modell vom gleichen Hersteller benutzt.
Im privaten Umfeld mag all dies zwar lästig, peinlich oder ärgerlich sein, existenzbedrohend ist es nicht. Im Unternehmensumfeld hingegen stellen derartige Schwachstellen eine echte Gefahr dar: Kaum auszumalen, was es für eine mittelständische Firma bedeutet, wenn ihre jüngste Neuentwicklung der Konkurrenz noch vor Veröffentlichung bekannt wird, nur weil die Steuerung einer Produktionsmaschine allzu schwatzhaft ist. Nötig sind in diesem Fall Vorkehrungen, die dafür sorgen, dass Geräte mit Zugriff auf derart sensible Informationen entweder vom Internet ganz getrennt werden oder dass der Zugriff aufs Internet streng reglementiert wird, so dass nur Zugriffe auf wirklich erforderliche Adressen möglich ist. Umgekehrt muss der Zugriff von außen so weit stark begrenzt werden, dass die

Arbeit im Unternehmen nicht gestört wird, aber dass auch kein versteckter Datenabfluss erfolgen kann.

Lösungen und Ansätze

Symantec z.B. liefert eine Lösung für Unternehmen, innerhalb der ein eigener Regelsatz für IoT existiert. Das Prinzip ist ziemlich einfach: Früher sperrte man den Webserver des Unternehmens in die DMZ (Demilitarized Zone), von der aus jeder Zugriff aufs Firmennetz verwehrt war, berechtigte Stationen aber auf den Webserver aus dem Firmennetz heraus zugreifen konnten. Ähnlich verfährt die Software nun auch mit IoT-Geräten: Die landen entweder im gleichen Netzsegment oder in eigenen Mikrosegmenten, so dass sie nur die für sie nötigen Internetadressen erreichen können – und möglichst keine weiteren Geräte innerhalb des Firmennetzes. Diese Kommunikation ist meist unnötig, weil die Stacks für die Produktionssteuerung selbst i.d.R. keine Daten produzieren, sondern nur mit solchen

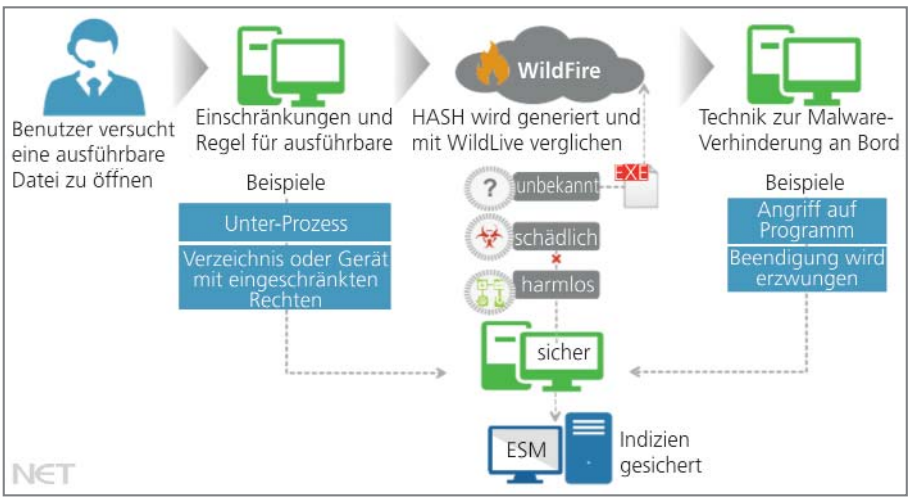

Bild 1: Schnelles Reagieren im Fall des Falles: Palo Alto Networks implementiert als Lösung ein engmaschiges Netz an Kontrollinstanzen, die Abweichungen von der Norm im Keim ersticken sollen

bestückt werden müssen, wenn sich an der Produktion etwas ändert.

Interessant ist auch der Ansatz, den die Sicherheitsfirma Tenable für ihre Verfahren nutzt, innerhalb von Unternehmen die Datensicherheit zu stärken. Der geht davon aus, dass es für jeden Angriff auf ein Netz eine Landkarte von Schwachstellen geben muss – quasi ein Google Maps für Hacker. Mit dieser Landkarte kann aber auch ein Sicherheitsdienstleister dafür sorgen, dass Hacker sich an den vermeintlichen Schwachstellen die Zähne ausbeißen.

Palo Alto Networks verfolgt einen Ansatz, der sowohl eine Absicherung des Internetzugangs mit einer modernen Firewall als auch des Netzes durch den Schutz und die Überwachung der Cli-

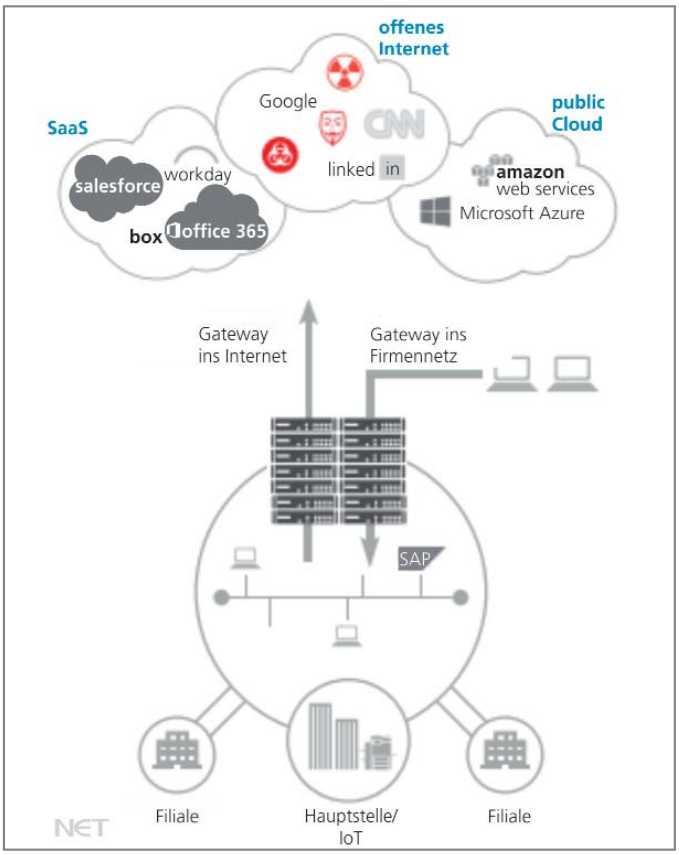

Bild 2: Bei Zscaler geht es darum, die Komplexität moderner Netze herunterzubrechen und sie einfacher und durchschaubarer zu gestalten, damit man einen effektiveren Schutz bieten kann

ents vorsieht (*Bild 1*). Das heißt, die Softwarelösung geht nicht davon aus, dass Clients innerhalb des Netzes von Haus aus sicher sind. Vielmehr heißt die Devise der Software: Vertraue niemandem, kontrolliere alle. Hinzu kommt eine Verhaltensanalyse, die verdächtige Aktivitäten im Netz erkennen und dann verhindern soll. Hier fließen die Erfahrungen aller Palo-Alto-Kunden mit ein, via Cloud werden auch die neuesten Verhaltensmuster für alle Kunden automatisch verfügbar. Der Vorteil: Die Erkennung neuartiger Angriffe gelingt so sehr viel schneller als mit den herkömmlichen Onlineupdates, wie sie viele Antivirenprogramme ausführen.

Fortinet baut auf mehrere Stützen, mit deren Hilfe Unternehmen ihre Datenverarbeitung sicherer gestalten können. Obenan steht wie bei Palo Alto eine hochmoderne Firewall zum Abblocken der meisten Zufallsangriffe. Der ganzheitliche Ansatz von Fortinet erstreckt sich aber nicht nur via Software bis zu den Clients, sondern bindet auch Hardware wie Switche und WLAN-Access-Points mit ein, um möglichst schnell verdächtige Verhaltensweisen im Netz aufzuspüren. Mit diesen Elementen sowie mit Informationen aus der Cyber Threat Alliance kann erheblich schneller und umfassender auf Bedrohungen reagiert werden.

Die Cyber Threat Alliance ist eine Gruppe von Unternehmen, die zusammenarbeiten, um in gegenseitigem Vertrauen Informationen auszutauschen, damit sie so gemeinsam schneller und besser auf diese Bedrohungen reagieren können, um ihre Kunden erfolgreicher zu schützen. Diese Organisation verfolgt mehrere Ziele. Zum einen will sie die Kunden der teilnehmenden Unternehmen schützen. Zum anderen will sie Angreifer mit Schadensabsichten identifizieren und dingfest machen. Indem die Allianz diese Ziele verfolgt, soll die Gesamtsicherheit von Unternehmensnetzen weltweit verbessert werden.

Cisco wiederum entwickelt sich mehr und mehr vom reinen Hardware- zum integrierten Software- und Hardwarehersteller, dessen Fokus sich hin zu Sicherheitsfunktionen für Netze aller Größen verschiebt. Dabei setzt der Konzern auf integrierte Lösungen, bei denen Hard- und Software aus dem Hause Cisco Hand in Hand zusammenarbeiten und maximalen Schutz gewährleisten. Insbesondere bei Angriffen durch Ransomware soll diese Architektur besonders wirksamen Schutz bieten. So sorgen Portsperren auf den Switchen dafür, dass der Schaden durch die Verschlüsselung nach dem Öffnen einer befallenen E-Mail minimiert wird. Bei Cisco gehört der Schutz von IoT-Geräten ins Netz – mit Firewalls und Mikrosegmentierung geht der Branchenprimus daran, die Netze seiner Kunden und die darin enthaltenen IoT-Geräte zu schützen.

Es klingt schon fast wie die Quadratur des Kreises, wenn ein Hersteller von einer Cloud-Security-Plattform spricht: Bislang fiel der Begriff Cloud i.d.R. nicht im Zusammenhang mit Sicherheit, sondern vielmehr im Zusammenhang mit Schwachstellen, staatlichen Hackversuchen und bekannt gewordenen Geheimnissen. Zscaler benutzt diesen Begriff, um zu beschreiben, wie eine Sicherheitslösung aus dem Portfolio dieser Firma aussehen soll (*Bild 2*). Die Experten des Unternehmens liefern ihre Erkenntnisse über neue Bedrohungen via Cloud in Echtzeit an alle Kunden aus, die diesen Service gebucht haben. Dabei geht man davon aus, dass die herkömmliche Firewall weitgehend ausgedient hat – zu unflexibel, zu teuer im Betrieb, zu wenig nützlich angesichts der Bedrohungen, die derzeit Unternehmensnetzen zu schaffen machen.

Gerade die Ansicht über Firewalls dürfte man bei Check Point Software nicht wirklich teilen, immerhin ist diese Firma auch heute noch der Inbegriff der leistungsfähigen, flexibel konfigurierbaren und sicheren Firewall. Doch damit tut man Check Point eigentlich Unrecht, denn schon lange hat die Firma ihr Portfolio um komplette Sicherheitslösungen erweitert. Vollständige Lösungen z.B. für den Gesundheitsbereich, für Service Provider, Regierungsbehörden und vieles mehr liefert sie aus. Doch dabei spielt grundsätzlich das Produkt „Firewall" eine wesentliche Rolle, weil sie dazu beiträgt, den Zugang zum Unternehmensnetz zu reglementieren, zu kontrollieren und zu schützen.

Was aber den einzelnen Herstellern abgeht: Keiner weiß so genau, wie die bislang installierte EDV-Landschaft im jeweiligen Unternehmen aussieht. Systemhäuser wie z.B. Controlware in Dietzenbach verfügen über dieses Detailwissen und können darauf aufbauend auch Lösungen implementieren, die nicht aus einer Hand stammen, sich aber in diesem Kontext perfekt ergänzen. *(bk)*