Pressemitteilung

IT-Security-Trends 2016: Explodierende Zahl an vernetzten Geräten stellt Unternehmen vor große Herausforderungen

Sicherheitsexperte EfficientIP erklärt, warum sich Firmen künftig verstärkt um eine robuste DDI-Basis kümmern sollten.

Eschborn, 03. Februar 2016 – Worauf müssen sich Unternehmen 2016 in Sachen IT-Security besonders einstellen? Ein Bereich, dem künftig wachsende Bedeutung zukommt, ist – so prognostizieren es die Sicherheitsexperten von EfficientIP – das Internet der Dinge (IoT). Denn die wachsende Anzahl vernetzter Geräte bietet nicht nur zahlreiche Möglichkeiten und Chancen, sondern eröffnet gleichzeitig neue Einfallstore für Hacker. So gehen die Analysten von Gartner beispielsweise davon aus, dass sich der IoT-Markt in den kommenden Jahren nahezu explosionsartig entwickeln wird. Bis 2020 wächst die Zahl der miteinander kommunizierenden Geräte demnach auf 25 Millionen. Das Problem laut EfficientIP: Auch Cyberattacken und das Ausmaß der Folgen eines derartigen Angriffs werden künftig rasant zunehmen.

Die Allgegenwärtigkeit und Zunahme von Dienstleistungen, vernetzten Geräten und Sensoren in Geschäften und Unternehmen stellt zweifelsohne ein signifikantes Sicherheitsproblem dar. Es finden sich zahlreiche Beispiele wie Überwachungskameras, Eingangsportale, Server, Software, Drucker oder auch Klimaanlagen, die Hackern günstige Gelegenheiten bieten. Da Geräte wie diese stets mit dem Internet verbunden sind, sind sie auch allen Gefahren, die das Internet betreffen, ausgesetzt. Die Herausforderung für Unternehmen besteht nun darin, sich dieser Thematik vermehrt zu widmen, denn bislang beschäftigen sich ihre Sicherheitsvorkehrungen nur unzureichend mit den vielen neuen Geräten und potenziellen Risiken – auch wenn sie künftig immer mehr zum Ziel für Hacker werden. Der aktuelle IBM 2015 Cyber Security Intelligence Index gibt in diesem Zusammenhang einen weltweiten Überblick über Vorfälle und Cyberangriffe auf operative Dienste. Ein interessantes Ergebnis ist hierbei, dass 30 Prozent aller Attacken und Sicherheitsvorfälle aus dem unternehmensinternen Umfeld kommen.

Doch wie gelingt es Cyberkriminellen, die Infrastruktur eines Unternehmens über das Internet der Dinge zu untergraben? Es gibt verschiedene Einfallstore, die es 2016 und darüber hinaus vermehrt zu beachten gilt: Angriffe von innen, Attacken von außen sowie Angriffe via DNS-Protokoll.

Hacker schmuggeln Daten durch das DNS-Protokoll

Öffnet ein Mitarbeiter eine firmeneigene oder öffentliche Webseite, durchlaufen alle Anfragen einen transparenten DNS-Server. So lassen sich unbemerkt Malware auf einem PC installieren und kleine Datenfetzen durch das DNS-Protokoll schmuggeln. Da sich die gestohlenen Daten in der Kapsel des DNS-Protokolls befinden, können die meisten Sicherheitstools sie nicht aufdecken: Das Protokoll scheint ein rechtmäßiger und legitimer Datenausgang zu sein, um eine Antwort von einem DNS-Server zu erhalten.

Aktuell im Einsatz befindliche Lösungen sind laut einer Umfrage der IDC nicht stark genug, um alle an sie gestellten Anfragen methodisch zu filtern. Oftmals beeinflusst diese Methode den DNS-Service sogar negativ, da sie unerlaubte Anfragen durchlässt wenn das System zu sehr unter Druck steht. Daher sind spezielle Lösungen für DNS-Services notwendig, die die unterschiedlichsten Angriffsarten entdecken und identifizieren können und entsprechende Gegenmaßnahmen einleiten.

Smart DDI garantiert verlässliche Automatisierung

Wer als „multi-vernetztes" Unternehmen in einer datenzentrierten und -dominierten Welt bestehen und nicht zur Zielscheibe von Cyberkriminellen werden möchte, sollte sich als guten Vorsatz fürs neue Jahr vornehmen, mehr Geräte als zuvor in die firmenweiten Sicherheitsüberlegungen miteinzubeziehen und DNS-Services besser abzuschirmen. Jede IT muss darüber hinaus eine robuste DDI Basis haben, auf der für das Unternehmen kritische Geschäftsvorgänge aufbauen. „Neue Anforderungen und eine dynamische Zukunft machen Smart DDI erforderlich", erläutert Ralf Geisler, Country Manager für die DACH-Region bei EfficientIP. Er fügt hinzu: „Die SMART DDI-Lösung von EfficientIP bietet ein umfassendes und integriertes Management von DNS/DHCP/IPAM und VLANs/VRF mit Devices und ihren Netzwerkschnittstellen in einem einzigen Prozess. Die SOLIDserver DDI Appliance definiert und verwaltet die komplexen Beziehungen zwischen allen IP-abhängigen Ressourcen. Diese ganzheitliche Lösung gewährleistet eine bisher unerreichte Automatisierung der DDI Deployment Prozesse und unterstützt so konkret die Geschäftsziele."

# # #

Über EfficientIP
EfficientIP ist ein internationaler Software-Hersteller für DDI-Lösungen (DNS, DHCP und IPAM - IP Address Management). Das Unternehmen vertreibt seine Produkte über ein weltweit agierendes Partnernetzwerk. EfficientIP ist in den wichtigsten Branchen wie Banken, Telekomanbieter, Industrie, Dienstleistungen und Behörden tätig. Als einer der führenden Anbieter im Markt nutzen hunderte der anspruchsvollsten Unternehmen die EfficientIP-Lösungen. Dazu gehören Unternehmen wie Vodafone, EADS, BskyB, Crédit Agricole, STMicroelectronics und T-Mobile.

EfficientIP hat das fortgeschrittene SmartArchitecture-Konzept entwickelt. Es hebt die Verwaltung von DNS und DHCP vom Service-Level auf die Architekturebene. EfficientIP bietet eine Reihe von leistungsfähigen Hardware- und virtuelle Appliances-Lösungen wie den SOLIDserver für IP Address Management, DNS- und DHCP-Management sowie Dienstleistungen. Für weitere Informationen besuchen Sie bitte: www.efficientip.com/de.

Pressekontakt:
LEWIS Communications

Mark Schüpstuhl
Tel: + 49 (0) 211 522946 0
efficient-ip@teamlewis.com