COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/hp-eroeffnet-deutsches-cyberabwehrzentrum,3044082

Schutzdienste im Baukastensystem

HP eröffnet deutsches Cyberabwehrzentrum

Datum: 15.12.2014
Autor(en): Michael Matzer

HP hat in Böblingen sein weltweit neuntes Cyberabwehrzentrum eröffnet. Kunden können einen umfangreichen Baukasten von Schutzdiensten mieten, unter anderem gegen DDoS-Angriffe. HP sieht die deutsche Industrie als besonders gefährdet an.

Das deutsche Cyberabwehrzentrum von Hewlett-Packard in Böblingen
Foto: Hewlett-Packard

Die 21 Mitarbeiter des Security Operations Centers (SOC) im schwäbischen Böblingen arbeiten im Schichtbetrieb und werden rund um die Welt von ihren 5.000 Kollegen in den acht anderen SOCs und im Forschungszentrum unterstützt. "Auf diese Weise ist ein Rund-um-die-Uhr-Betrieb gewährleistet", erklärt Claudio Wolff, der Leiter des Zentrums. **HP**[1] Enterprise Security Services schützt zur Teit weltweit 47 Mio. Nutzerkonten. In das Cyberabwehrzentrum Deutschland habe HP jedenfalls "eine zweistellige Euro-Millionensumme" investiert, so Ralf Brunner, Leiter der IT Services Delivery für Zentral- und Osteuropa.

Zielgruppen

Claudio Wolff, Leiter des Cyberabwehrzentrums von HP in Böblingen.
Foto: Hewlett-Packard

Das Angebot des HP-Cyberabwehrzentrums richtet sich an mittelständische und große Unternehmen sowie an öffentliche Einrichtungen. Durch seine Nutzung sparen sie fortlaufende Trainingskosten für eigene IT-Sicherheitsexperten und Investitionskosten für IT-Sicherheitstechnik ein und sind trotzdem auf die neuen Angriffstypen und Sicherheitsbedrohungen vorbereitet. Außerdem versetze es die Nutzer im Falle eines Schadenfalles in die Lage, anhand von IT-Forensik handfeste digitale Beweise zu sammeln. Diese sind laut Wolff vonnöten, um vor Staatsanwaltschaft und Versicherung nachweisen zu können, dass überhaupt ein Angriff stattgefunden hat und ein Schaden entstanden ist.

Milliardenwerte

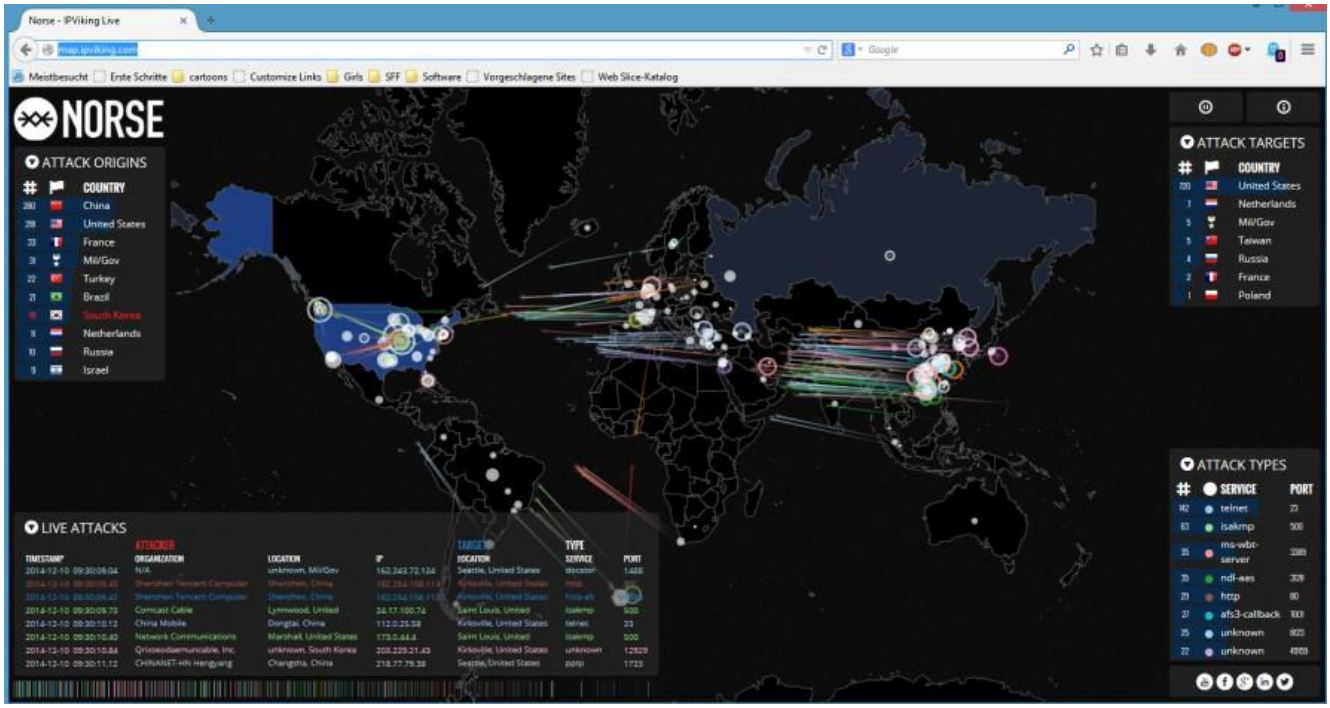


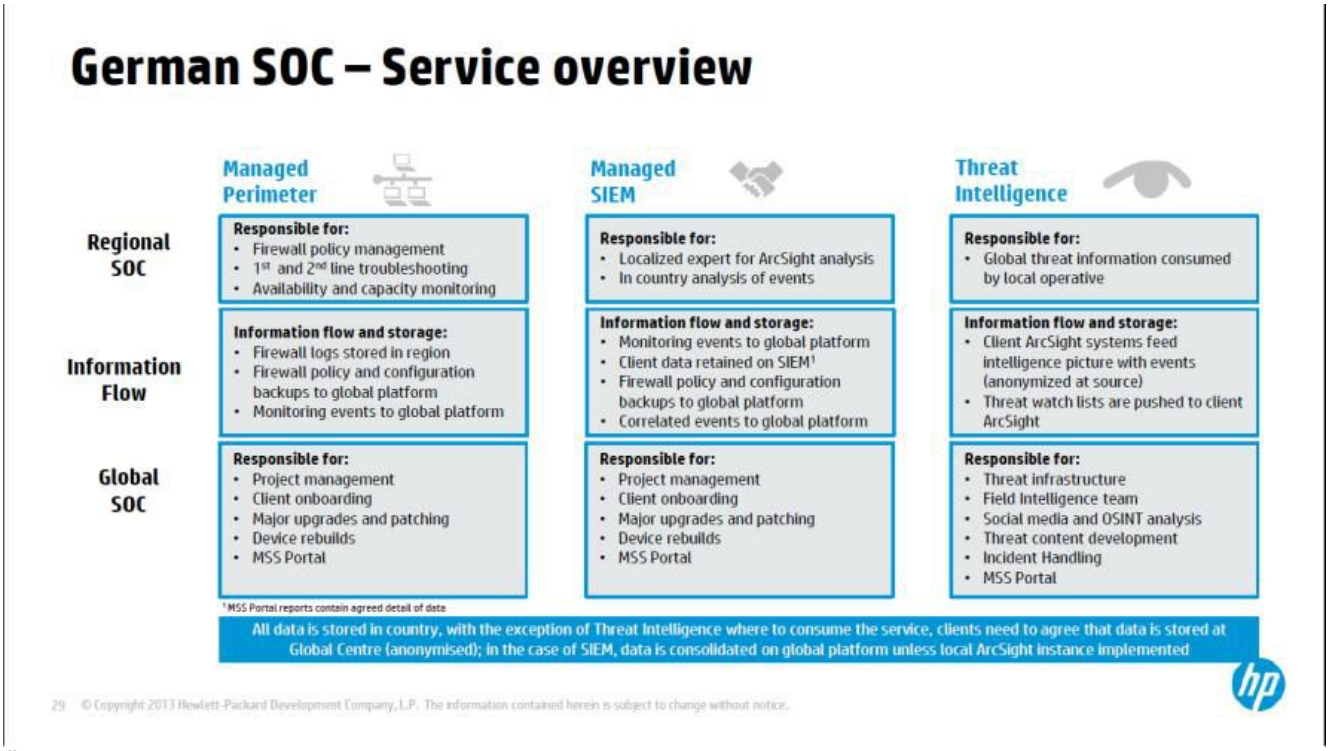
Abb. 6. Einer der Bildschirme im HP-Cyberabwehrzentrum zeigt in Echtzeit, welche Angriffe in aller Welt über das Internet geführt werden. Die Darstellung lässt sich bei Norse-IP-Viking finden.
Foto: Michael Matzer

Bei den Cyberangriffen geht es um Milliardenwerte. 46 Mrd. Dollar investieren die Unternehmen weltweit in IT-Sicherheit, laut Wolff rund 8 bis 9 Prozent ihres IT-Budgets. Doch jeder erfolgreiche Angriff "kostet ein deutsches Unternehmen laut Ponemon Institute im Schnitt 8,13 Millionen Dollar, und es dauert 21 Tage, um einen Cyberangriff unter Kontrolle zu bekommen", sagte Arthur Wong, der Chef der Abteilung für Unternehmenssicherheit bei HP, bei der Eröffnung des Böblinger Cyberabwehrzentrums.

Funktionsumfang

Arthur Wong ist Senior Vice president und Global General Manager der Enterprise Security Group bei HP. Er war zuvor bei Symantec und McAfee.
Foto: Hewlett-Packard

Eines der Systeme analysiert laufend sicherheitsrelevante Systemdaten, um Sicherheitsbedrohungen frühzeitig aufzuspüren. Eine weitere Software überwacht unstrukturierte Informationsquellen im Internet, um neue Angriffstypen oder konkrete Angriffe bereits in einem frühen Stadium zu erkennen. Andreas Wuchner, Security CTO und Sicherheitsexperte bei HP, sagte: "Mit diesen Programmen können wir bereits wahrscheinliche Angriffsziele voraussagen." Das Böblinger Cyberabwehrzentrum erhält seine Informationen über neue Sicherheitsschwachstellen laufend aus dem weltweiten HP-Sicherheitsnetz.



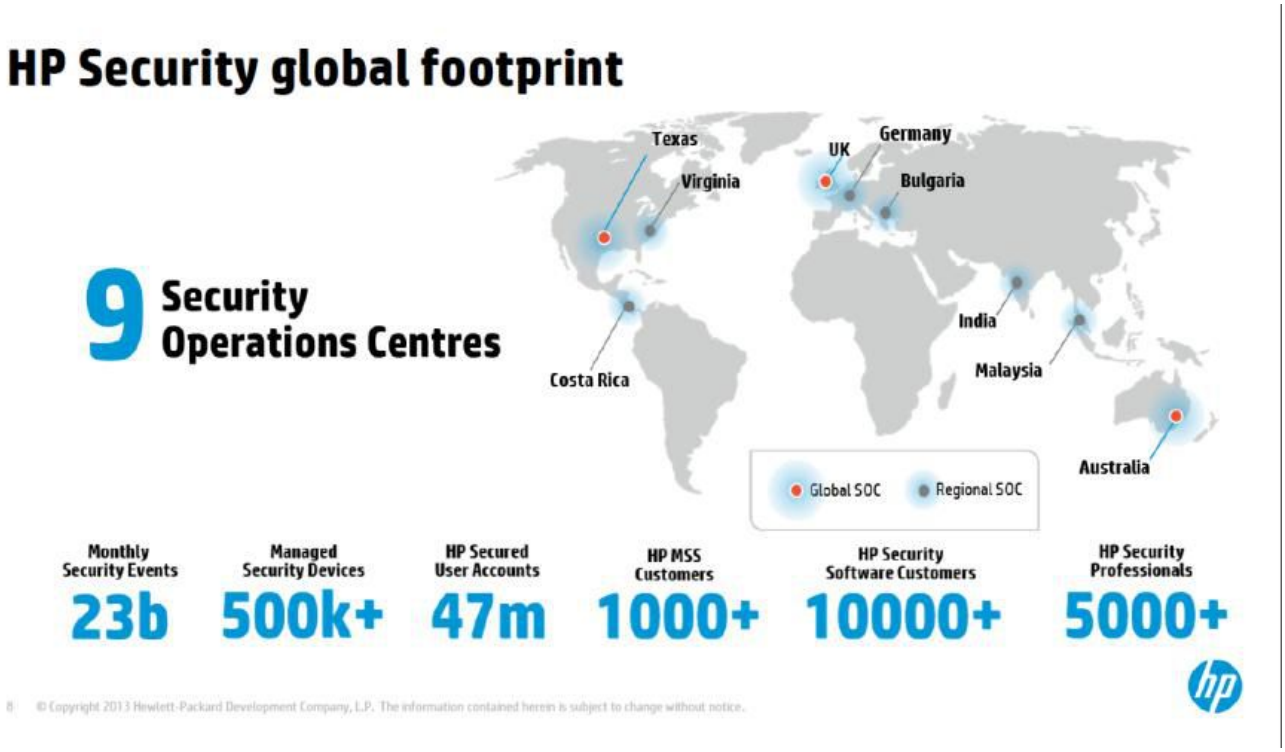
Übersicht der Dienste, die das German SOC von Hewlett-Packard erbringen kann.
Foto: Hewlett-Packard

Zu den Angriffsmethoden, die das Böblinger SOC abwehren kann, gehören laut Wuchner auch Distributed Denial of Service (DDoS) Attacken mithilfe von Botnetzen. Deren Anzahl und Wucht nimmt rasant zu und dient gerade in der Weihnachtszeit dazu, Webshops zu erpressen. Der Schutz vor DDoS ist nur ein Baustein, den ein Kunde aus dem Baukasten von HPs Sicherheits-Suite individuell auswählen kann.

Globale Aufstellung, lokaler Einsatz

Die Mitarbeiter des SOC arbeiten auf vier Ebenen.
Foto: Hewlett-Packard

Der Vorteil des HP-SOC liegt laut Wong in dem Fachwissen, der Kompetenz, der globalen Aufstellung und der schnellen Reaktionszeit von HP. "Die Angreifer sind global vernetzt und spezialisiert; wir müssen ebenfalls global vernetzt sein, um das nötige Wissen für die Abwehr zu erlangen. Aber wir müssen lokal handeln, um innerhalb der jeweiligen Landesgesetze tätig werden zu können", so Wong.



Die HP-Sicherheitsorganisation ist global aufgestellt.
Foto: Hewlett-Packard

HPs Maßnahmen zur Vorbeugung gegen und Abwehr von Bedrohungen müssen mit den jeweils lokal herrschenden Gesetzen in Einklang stehen. Indem es diesbezüglich auf deutsche Rechtsberater zurückgreift, will das Unternehmen Konflikte mit Betriebsräten vermeiden, so Claudio Wolff, der Leiter des Böblinger Abwehrzentrums. Es geht nicht an, dass man unerlaubt einen Mitarbeiter überwacht, nur weil dieser verdächtige Aktivitäten an den Tag legt.

Deutschland ist laut Ponemon Institute ein bevorzugtes Ziel der Angreifer und zahlt pro erfolgreicher Attacke einen hohen Preis.
Foto: Hewlett-Packard

Weitere Gründe, nach Deutschland zu kommen, sind nach Wongs Angaben die hohe Gefährdung des herausragenden Industriestandorts Deutschland, die infolgedessen hohe Nachfrage nach Datenschutz und Datensicherheit, aber auch das gute Angebot von qualifiziertem Personal in Zentraleuropa.

"Security-Experten sind weltweit rar geworden", berichtet Wong, "und wir gehen dorthin, wo wir sie bekommen können." Ausdrücklich ruft der Abteilungschef die deutschen Universitäten, Unternehmen und vor allem Partner auf, ihr Personal zur Aus- und Fortbildung zu HP Enterprise Security Services zu schicken. In Böblingen erhalten sie Anschauungsunterricht, welche begehrten Schlüsselpositionen sie erlangen können. (rw)

Links im Artikel:

[1] **http://www.hp.com**
