Link: https://www.cio.de/a/it-security-an-den-richtigen-stellschrauben-drehen,2976698

Mehr Sicherheit für Daten und Netzwerke

IT-Security: An den richtigen Stellschrauben drehen

Datum: 14.11.2014
Autor(en): Stefan Gneiting

Unternehmen müssen ihre Investitionsstrategie für die Netzwerk- und Datensicherheit überdenken. Ein Gespräch mit Jürgen Seiter, Leiter Security Services Business bei HP Deutschland, über Bedrohungén für Unternehmensnetzwerke und wie man ihnen am besten begegnet.

Zum dritten Mal erschien vor kurzem die **"2014 Cost of Cyber Crime Study: Germany"**[1]. Sie wurde vom US-amerikanischen Ponemon Institute durchgeführt und von Hewlett Packard finanziert. Die Analyse der Schäden und Kosten durch Cyber-Kriminalität soll den Verantwortlichen in den Unternehmen helfen, die notwendigen Investitionen in die Sicherheit der Unternehmensnetzwerke und die Datensicherheit zu optimieren. Jürgen Seiter, Leiter Security Services Business D,A,CH und Osteuropa bei HP, erläutert im Interview die Erkenntnisse aus der Studie.

Jürgen Seiter, Leiter Security Services Business HP Deutschland: "Hacker werden immer raffinierter."
Foto: HP Deutschland

Die Ponemon-Studie "2014 Cost of Cyber Crime" fand heraus, dass die Schäden, die deutsche Unternehmen durch Cyber-Attacken erleiden, steigen. Vernachlässigen die IT-Verantwortlichen die IT-Sicherheit?

Jürgen Seiter: Nein, so pauschal kann man das nicht sagen. Einerseits steigt der Wert der Daten durch die Digitalisierung in den Unternehmen stetig an. Das heißt, dass der Verlust von oder der unerlaubte Zugriff auf Daten finanziell stärker ins Gewicht fallen. Und die Abhängigkeit der Unternehmen von einer funktionierenden IT nimmt ebenfalls zu. Zum anderen werden die Hacker immer raffinierter, sind immer besser organisiert und greifen viel gezielter an als früher.

Bedeutet das, dass die Unternehmen die IT-Security-Kosten weiter hochfahren müssen?

Jürgen Seiter: Höhere Budgets helfen nicht weiter, wenn man an den falschen Stellschrauben dreht. Es geht vor allem darum, die richtigen Investitionen zu tätigen. Die erwähnte Ponemon-Studie hat gezeigt, dass in diesem Jahr erstmals Phishing und Social Engineering - der Diebstahl von Identitäten und das Erschleichen von persönlichen Daten durch soziale Manipulation - in großen Unternehmen die höchsten Folgekosten verursachen.

Darauf sind viele unzureichend vorbereitet. Sie sollten bei den Security-Investitionen auch die Kostenverursacher im Blick haben. Maßnahmen zur Verbesserung der Applikations-Sicherheit und in Schulung der Mitarbeiter stehen nicht ganz oben auf der Prioritätenliste der IT-Verantwortlichen. Hier muss ein Umdenken stattfinden.

Also weniger Investitionen in Netzwerk-und Datensicherheit, mehr Geld für Mitarbeiterschulungen und Anwendungssicherheit?

Jürgen Seiter: Man muss zielgerichtet investieren und darf keinen Sicherheitsaspekt außer Acht lassen. Man muss die richtige Balance zwischen Netzwerk-, Daten-, Anwendungs- und Gerätesicherheit sowie Mitarbeiterschulung finden. Vor allem darf man sich nicht zurücklehnen. Sicherheit ist ein ständiger Prozess.

Eine Firewall allein reicht schon längst nicht mehr als Sicherheitskonzept aus, da diese nur auf Angriffe reagiert. Man muss aber proaktiv agieren. Die Angreifer sind sehr flexibel und erfindungsreich. Hier muss man immer am Puls der Zeit bleiben. HP betreibt beispielsweise acht Security Operations Centers, die ständig das weltweite Security-Geschehen verfolgen und darauf basierend neue Sicherheitsdienstleistungen entwickeln und anbieten.

Security-Intelligence-Systeme sind effektiv

Welche konkreten Maßnahmen empfehlen Sie den IT-Verantwortlichen, um Schäden durch Attacken auf die IT-Infrastruktur zu verhindern oder zumindest zu verringern?

Jürgen Seiter: Wie Sie bereits erwähnt haben, ist die Schulung zur Sensibilisierung der Mitarbeiter äußerst wichtig. Interne Angriffe - ob absichtlich oder unabsichtlich unterstützt- sind sehr schwer zu entdecken und damit auch schwer zu beheben. Wie die Ponemon-Studie zeigt, bringt der Einsatz von Security-Intelligence-Systemen die größten absoluten Einsparungen von Cyberkriminalitätskosten. Das zweitgrößte absolute Einsparpotenzial liegt in der umfangreichen Nutzung von Verschlüsselungs-Technologien. Beim Return on Investment liegen diese beiden Technologien ebenfalls vorne.

Sind kleinere Unternehmen bzgl. der Security schlechter aufgestellt als große?

Jürgen Seiter: Die absoluten Schäden durch Cyberkriminalität steigen naturgemäß mit der Mitarbeiterzahl. Berechnet man aber die Kosten pro Kopf, dann stehen große Unternehmen besser da als die kleinen.

Die größten Unternehmen in der Ponemon-Studie hatten Kosten von 442 Euro pro IT-Arbeitsplatz, die kleinen dagegen von 1354 Euro. Kleine Firmen müssen sich anders aufstellen als große Konzerne.

Es zeigt sich, dass kleinere Organisationen die höchsten Kosten durch auf Geräten eingeschleuste Viren, Würmer und Trojaner, durch Gerätediebstahl sowie durch Schadsoftware im Unternehmensnetzwerk entstehen. Bei größeren Unternehmen hingegen sind die Schäden aus Angriffen aus dem Internet, Phishing und Social Engineering sowie durch Angriffe von innen, also von Mitarbeitern oder Partnern verschuldete Attacken, am höchsten.

Was entgegnen Sie denjenigen, die behaupten, dass kleinere Organisationen weder den finanziellen noch den personellen Aufwand für die Umsetzung eines umfassenden Sicherheitskonzepts leisten können und daher immer anfälliger gegen Cyberangriffe sein werden.

Jürgen Seiter: Das stimmt so nicht. Wer nicht die Assets für die Realisierung eines Sicherheitskonzepts hat, sollte die Security in die Hände von spezialisierten Experten legen. Das Security-Outsourcing ist heute bereits weit verbreitet und lässt sich einfach und relativ kostengünstig realisieren.

Das Sparen an der falschen Stelle wird sich unweigerlich negativ auswirken. Die Folgekosten erfolgreicher Angreife auf die IT übersteigen meist die Investitionen für eine wirksame Abwehr. Man darf auch nie außer Acht lassen, dass neben den direkten Kosten auch erhebliche, langfristige Einbußen durch den Reputations- und Imageverlust entstehen können.

Anscheinend ist heute kein Unternehmen davor gefeit, Opfer einer Cyber-Attacke zu werden. Was ist zu tun, wenn der Fall der Fälle eingetreten ist?

Jürgen Seiter: Nach der Entdeckung des erfolgreichen Angriffs darf man keine Zeit verlieren und muss die Einfallstore schnellstmöglich schließen. Möglicherweise ist es sinnvoll, qualifizierte Hilfe von außen zu holen. Aber mit der Beseitigung der Schwachpunkte ist es nicht getan. Man sollte eine eingehende Analyse machen, wieso die Hacker eindringen konnten und darauf basierend eine Strategie entwickeln, die vor künftigen Zwischenfällen besser schützt.

Links im Artikel:

[1] **https://ssl.www8.hp.com/us/en/ssl/leadgen/secure_document.html?objid=4AA5-5207ENW&siebelid=12503&sectionid=pdf&returnurl=/us/en/secure/pdf/4aa5-5207enw.pdf&simpletitle=ponemon%20cyber%20report&subbu=tsg.software&parentPageName=3.0&analytics_page_name=3.0&parentUrl=http%**
solutions/ponemon-cyber-security-report/index.html%3Fjumpid%3Dva_mq32xtevyi%26jumpid%3Dreg_r1002_usen_c-001_title_r0001&compURI=tcm%3A245-1788580&fv=FLEX2%20SW3&metrics_asset_value=eb&bu=tsg&st=/us/en/software-solutions/ponemon-cyber-security-report&as=software&wsi=r11374&cu=false

---

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.