"Die eBay-Attacke ist kein Einzelfall

"Die eBay-Attacke ist kein Einzelfall"

Kommentar zum eBay-Angriff von Lucas Zaichkowsky, Enterprise Defence Architect für den Vertrieb von Problembehebungstechnologien bei AccessData
Es ist noch nicht lange her, da teilte eBay mit, dass das Unternehmen mit den Behörden der Strafverfolgung zusammenarbeitet und die besten forensischen Tools und Methoden einsetzt, um seine Kunden zu schützen. Und doch vergingen nach dem ersten Cyberangriff drei Monate, bis dieser ans Licht kam, und weitere 14 Tage, bis nach der Untersuchung und den Reparaturen die Bekanntmachung gegenüber den Kunden erfolgte. Die eBay-Attacke ist jedoch kein Einzelfall.
Anfang des Jahres haben AccessData und die Marktforscher des Ponemon Institute 1.083 Chief Information Security Officer (CISOs) befragt, was ihre Unternehmen unmittelbar nach einem Cyberangriff tun und was unternommen werden könnte, um die Reaktions- und Reparaturzeiten zu verkürzen. 86 % der Befragten antworteten, dass die Erfassung von Cyberangriffen zu lange dauere. 38 % berichteten, dass es ein Jahr dauern könne, bis die Ursache einer Störung festgestellt sei, während 41 % angaben, dass sie die Ursache niemals finden würden.
Wenn eine Datenpanne identifiziert ist, macht es die fehlende Verzahnung der verschiedenen Sicherheitsüberwachungsprodukte für Security-Experten sehr schwer, sich durch die große Menge von Warnmeldungen und Daten zu kämpfen, die betroffenen Knotenpunkte zu isolieren und die Ursache einer Störung zu lokalisieren. Es bestehen Zweifel, ob Unternehmen eine obligatorische Bekanntgabe für schwere Datenpannen innerhalb von 24 Stunden umsetzen können, wie es die EU-Datenschutz-Grundverordnung nahelegt.
Cyberangriffe werden zu spät entdeckt
In einer Studie der Marktforscher des Ponemon Institute vom Februar 2014 mit dem Titel "Threat Intelligence and Incident Response: a study of US and EMEA organizations [Bedrohungsintelligenz und Störungsreaktion: eine Studie von US- und EMEA-Unternehmen] wurde Folgendes herausgefunden:

- 86 Prozent der Teilnehmer sind der Meinung, dass die Erfassung von Cyberangriffen zu lange dauert

- 85 Prozent der Teilnehmer berichten, dass sie es schwierig finden, Störungen zu priorisieren

- 61 Prozent der Teilnehmer beklagen, dass zu viele Warnungen verschiedener Sicherheitsprogrammen die Untersuchung behindern

- 74 Prozent der Teilnehmer sagen, dass eine fehlende Verzahnung der verschiedenen Einzellösungen für den Schutz und die Überwachung des Netzwerks die Reaktion auf Cyberstörungen verlangsamt

- 38 Prozent der Teilnehmer behaupten, dass die Feststellung der Ursache einer Störung ein Jahr dauern kann

- 41 Prozent der Teilnehmer sagen, dass sie niemals in der Lage seien, die Ursache mit Sicherheit zu identifizieren, was darauf hindeutet, dass die Sicherheitsabwehrsysteme weitere Angriffe derselben Virenüberträger nicht verhindern können

- 86 Prozent der Teilnehmer finden es schwierig, mobile Geräte zu untersuchen, wobei 54 Prozent berichten, dass sie nicht in der Lage bzw. unsicher sind, sensible Daten auf mobilen Geräten zu suchen

- 59 Prozent der Befragten sagen, dass sie die Bedrohungsanalyse mit ihren bestehenden Sicherheitslösungen nicht effektiv nutzen können; 40 Prozent berichten, dass sich mit keinem ihrer Sicherheitsprodukte Bedrohungsanalysen aus anderen Quellen importieren lassen.
Mit einer gestiegenen Anzahl von genutzten Mobilgeräten, angetrieben vom BYOD-Trend, sind mobile Daten für Security- und Rechtsabteilungen nun eine entscheidende Beweisquelle im Bereich e-Discovery geworden. Mobile Informationen aus Applikationen, SMS-Texten
 Co. schaffen ein besseres Verständnis bei Datenvorfällen und -ermittlungen. Ohne die Fähigkeit, die mobilen Daten schnell zu sammeln und zu analysieren, können Rechts- und IT-Abteilungen ihre Digital Investigations- und Litigation-Prozesse nicht effektiv erledigen.
Über AccessData:
Die AccessData Group ist seit 25 Jahren Wegbereiter für Entwicklungen im Bereich der digitalen Ermittlungen und entsprechender Unterstützung in Rechtsstreitigkeiten. Die Produktfamilie besteht aus Stand-Alone- und Enterprise-Class-Lösungen mit dem Fokus auf Digital Forensik, E-Discovery und Cyber Security. Hierzu gehören unter anderem die Produkte FTK, SilentRunner, Summation und das CIRT Security Framework. Sie ermöglichen digitale Untersuchungen jeder Art, wie z.B. Computerforensik, Vorfallsanalyse, Hosted Review Services, rechtliche Nachprüfungen und Compliance-Audits. Mehr als 100.000 User, die weltweit im Gesetzesvollzug, in Regierungsbehörden, Unternehmen und Rechtanwaltskanzleien etc. tätig sind, vertrauen bereits auf die AccessData Software-Lösungen. AccessData ist zudem Anbieter für Trainings und Zertifizierungen in den Bereichen digitale Forensik und Rechtsstreitigkeiten. Weitere Informationen unter www.accessdata.com .

Weitere Informationen:
AccessData Group
Nicole Reid
International Marketing Manager
1 Bedford Street
3rd Floor
London
E-Mail: nreid@accessdata.com
Internet: www.accessdata.com
Ansprechpartner (in Deutschland):
Abdeslam Afras
Director, EMEA
 India
E-Mail: aafras@accessdata.com
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
  www.sprengel-pr.com
Ansprechpartner:
Olaf Heckmann
Marius Schenkelberg
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: ms@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=566143" width="1" height="1">

Pressekontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Firmenkontakt

AccessData Group

84042 Lindon, UT

nreid@accessdata.com

Weitere Informationen finden sich auf unserer Homepage