85 % der IT-Security-Experten finden nicht alle Sicherheitslücken auf Mobilgeräten

85 % der IT-Security-Experten finden nicht alle Sicherheitslücken auf Mobilgeräten

Studie von AccessData und dem Ponemon Institute: Reaktion auf Cyber-Angriffe in den USA und EMEA nur mangelhaft
e-Discovery-Experte AccessData und die IT-Forscher des Ponemon Institute haben Studien zu Digital Investigations-Prozessen durchgeführt: 85 % der befragten CISOs (Chief Information Security Officer) in den USA und EMEA empfinden das Untersuchen von Mobilgeräten als diffizil. Die Hälfte aller Teilnehmer outet sich als nicht fähig bzw. unsicher beim Auslesen von Daten aus Smartphones
 Co. Auf die Frage nach der Reaktion auf Cyber-Angriffe gestand eine alarmierende Zahl von 41 % der CISOs, dass sie nicht in der Lage seien, die Ursache des Security-Vorfalls herauszufinden. Dies liegt vielerorts an der mangelnden Integration von Threat Intelligence.
Ein Teil der Studie des Ponemon Institutes beschäftigte sich mit einer großen Herausforderung von CISOs: Das Untersuchen von Daten- und Sicherheitsvorfällen bei Mobilgeräten. Wie funktionieren diesbezüglich die e-Discovery-Prozesse im Security-Team? Über die Hälfte der 1.083 befragten CISOs und Security-Techniker waren entweder nicht in der Lage oder unsicher, wie man solche Analysen auf mobilen Geräten durchführt. Sensible Daten wie Geschäftsgeheimnisse und personenbezogene Informationen können sie nicht von mobilen Geräten herausfiltern. Als passende Problemlösung sehen drei Viertel der Befragten eine kombinierte Security-, Internal Investigations- und e-Discovery-Plattform, die sich nahtlos in die Firmenstrukturen einfügt.
Reaktion auf Cyber-Angriffe suboptimal
Der zweite Teil der Befragung fokussierte sich auf die unmittelbaren Folgen von Cyber-Angriffen. Zunächst ging es um die allgemeinen Schwachpunkte bei Cyber Security- und Incident Response: 86 % der CISOs dauert der Nachweis einer Cyber-Attacke zu lange; 85 % leiden an mangelnder Priorisierung von Sicherheitsvorfällen; 74 % sprechen von einer schlechten oder keiner Integration verschiedener Security-Produkte; 61 % beklagen, dass zu viele Alarme der verschiedenen Einzellösungen die Untersuchungen behindern. Alle dieser Gründe schränken die Reaktionsfähigkeit auf Sicherheitsvorfälle ein.
41 % finden nie die Ursache
Darüber hinaus berichteten viele der Befragten von Problemen bei der Ursachenforschung einer Cyber-Bedrohung. 66 % der CISOs sind der Meinung, dass das Wissen über die Ursache des Vorfalls ihre Abwehr gegen Bedrohungen verstärkt Allerdings teilten 38 % der Security-Experten mit, dass sie oftmals bis zu einem Jahr brauchen, um den Ursprung einer Bedrohung zu finden. Besonderes alarmierend: 41 % der CISOs gaben zu, niemals die Ursache von Security-Vorfällen rauszufinden.
Integrierte Threat Intelligence ist ein vielversprechender Ansatz, um z.B. Mobilgeräte schneller zu untersuchen und Bedrohungen besser zu erkennen. Allerdings scheinen dies aktuelle Security-Produkte kaum aufzuweisen, wie die Studie zeigt: 59 % der Befragten sind nicht in der Lage, Threat Intelligence mit ihren existierenden Security-Produkten effektiv zu nutzen. 40 % der CISOs berichten, dass keine ihrer Sicherheitslösungen Threat Intelligence aus anderen Quellen importiert.
"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", erklärt Craig Carpenter, Chief Cybersecurity Strategist bei AccessData. "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."
Dr. Larry Ponemon, Vorsitzender und Gründer des Ponemon Institute erläutert abschließend: "Die Umfrage zeigt klar, dass e-Discovery-Prozesse eine leistungsfähige, intuitive Technologie benötigen, mit der Teams ihre Untersuchungen umfassend und effizient durchführen können. Das spart Zeit, Ressourcen und Geld für Unternehmen und Kunden."
Mehr Informationen zu den Cyber Security-, Digital Forensics-, Litigation- und e-Discovery-Lösungen von AccessData sind unter www. accessdata.com zu finden.
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
E-Mail: nreid@accessdata.com
Internet: www.accessdata.com
London
Ansprechpartner (in Deutschland):
Abdeslam Afras
Regional Manager Continental Europe
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_=560854" 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