## Neue IBM Studie: zu viele Sicherheitslücken in mobilen Apps und Geräten

Neue IBM Studie: zu viele Sicherheitslücken in mobilen Apps und Geräten<br /><br />- Gemeinsame Studie von IBM und dem Ponemon Institut<br />- Unternehmen sind zu leichtsinnig<br />- Mangelhafter Schutz bei mobilen Geräten / neue IBM Lösungen gegen mobile Malware <br />Eine gemeinsame Studie von IBM (NYSE: IBM) und dem Ponemon Institut kommt zum Ergebnis, dass mobile Applikationen und Geräte gravierende Sicherheitsmängel aufweisen. Fast 40 Prozent der größeren Unternehmen, darunter viele aus der Fortune-500-Liste, kümmern sich zu wenig um die notwendigen Sicherheitsvorkehrungen bei der Entwicklung mobiler Apps für ihre Kunden. Zudem sind sowohl die unternehmenseigenen mobilen Geräte wie auch private Geräte der Mitarbeiter, die für Geschäftszwecke genutzt werden, zu wenig geschützt. Sie bieten damit ideale Einfallstore für Cyberattacken auf Unternehmens-, Kunden- und private Nutzerdaten.<br />Die Anzahl mobiler Cyberattacken wächst kontinuierlich. Zu jedem beliebigen Zeitpunkt werden weltweit über 11,6 Millionen mobile Geräte infiziert (1). Das Ponemon Institut hat daher gemeinsam mit IBM die Sicherheitspraktiken in über 400 großen Unternehmen untersucht - mit einem alarmierenden Ergebnis: Ein durchschnittliches Unternehmen überprüft weniger als die Hälfte seiner Apps auf Sicherheitsmängel. Rund ein Drittel testen die Sicherheit ihrer Apps überhaupt nicht und schafft damit gleichsam eine ganze Armada von Zugangsmöglichkeiten über ungesicherte mobile Geräte. Das ist zwar schockierend, aber nicht weiter überraschend, denn die Hälfte der untersuchten Unternehmen plant bisher keinerlei Budget für Maßnahmen zur mobilen Sicherheit.<br />"Es fehlt in den Unternehmen bisher das Bewusstsein dafür, Sicherheit auch in mobile Applikationen einzubauen", sagt Gerd Rademann, Business Unit Executive IBM Security Systems DACH. "Damit wird Cyberkriminellen Tür und Tor geöffnet. Unternehmen müssen dringend lernen, mit vergleichbar effektiven Waffen zurückzuschlagen, mit denen sie heute attackiert werden."<br />Hacker nutzen mit Vorliebe unsichere mobilen Apps sowie öffentliche WLAN-Netzwerke, um auf Daten zuzugreifen, die immer häufiger direkt auf den mobilen Geräten abgelegt werden. Oder sie nutzen Apps als Einfallstor, um in das vertrauliche interne Netzwerk der Unternehmen vorzudringen.<br />Um sich gegen solche Angriffe besser zur Wehr setzen zu können, wurde die Expertise von IBM Security-Spezialisten aus dem Bereich Trusteer in die mobile Welt übertragen. Diese Experten kümmern sich gezielt mit dem Schutz sensibler Daten in komplexen Organisationen wie etwa Banken.<br />Alarmierende Schwachstellen<br />Die aktuelle Studie hat vier fundamentale Sicherheits-Schwachstellen bei der Entwicklung und Verbreitung mobiler Applikationen in den untersuchten Unternehmen identifiziert:<br />- Zu wenig Budget: Die untersuchten Unternehmen investierten durchschnittlich 34 Millionen US-Dollar jährlich in die Entwicklung mobiler Anwendungen. Davon fließen bei der Hälfte nur rund 5,5 Prozent in das Thema Sicherheit, satte 50 Prozent stellen für den Schutz ihre mobilen Apps gegen Cyberattacken keinerlei Budget bereit.<br />- Fehlende Überwachung: Um ihre Apps möglichst schnell und unterbrechungsfrei für Kunden verfügbar zu machen, neigen Unternehmen dazu, ihre Apps zu selten, zu spät und wenn überhaupt, dann auch nur unregelmäßig auf Sicherheitsmängel hin zu überprüfen. Diese fehlende Überwachung erlaubt Cyberkriminellen den nahezu ungehinderten Zugriff auf vertrauliche Geschäfts- und Personendaten. Allein 2014 wurden bei Cyberattacken über eine Milliarde persönlicher Daten erbeutet (2).<br />- Im Zweifel für eine höhere Nutzerfreundlichkeit: Bei der Entwicklung mobiler Applikationen geht Nutzerfreundlichkeit oft über Sicherheit und Datenschutz. Laut Studie gaben 65 Prozent der Unternehmen zu, dass sie Sicherheit im Interesse der Bequemlichkeit für ihre Kunden häufig zurückstellen. Für 77 Prozent ist außerdem der Zeitdruck bei der Markteinführung die wichtigste Ursache für sicherheitsrelevante Schwachstellen. <br />- Seltene Checks: Bei denjenigen Unternehmen, die ihre Apps auf Schwachstellen überprüfen noch bevor sie verbreitet werden, testen nur 15 Prozent regelmäßig, ob die Sicherheitsvorkehrungen noch effektiv greifen.<br />Je mehr private Geräte, desto höher das Risiko<br />Bring Your Own Device (BYOD), die Nutzung privater mobile Geräte, wird nicht nur immer populärer, sondern für viele Unternehmen sogar unverzichtbar. Dies wird immer dann zu einer Herausforderung, wenn Mitarbeiter sich mit unsicheren Netzwerken verbinden oder schlecht geschützte Apps von unsicheren Quellen herunterladen, die das Gerät verwundbar machen. Aber selbst große, bekannte Unternehmen und Organisationen, deren Apps scheinbar über jeden Zweifel erhaben sind, können enorme Risiken bergen, wie die Untersuchung zeigt.<br />Laut der Studie sind die meisten Mitarbeiter der befragten Unternehmer "heavy user" von mobilen Apps, dennoch sagen über die Hälfte (55 Prozent), dass ihre Organisation keine Vorschriften oder Richtlinien für deren Nutzung am Arbeitsplatz etabliert hat. Die überwiegende Mehrheit (67 Prozent) erlaubt zudem das Herunterladen auch nicht überprüfter Apps auf mobile Arbeitsgeräte, 55 Prozent das Herunterladen von Geschäftsanwendungen auf private Geräte (BYOD).<br />IBM MobileFirst unterstützt mobiles Threat Management<br />Um die Sicherheitsgefahren des mobilen Geschäfts auf ein Minimum zu reduzieren, hat IBM eine neue intelligente "Mobile Threat Management"-Technologie entwickelt (MTM). Als Bestandteil von IBM MobileFirst Protect ist das IBM MobileFirst Protect Threat Management speziell darauf ausgerichtet, verdächtige Aktivitäten an mobilen Endpunkten zu entdecken und Malware im Moment des Angriffs zu stoppen. Über die Cloud verfügbar und jederzeit mobil updatebar, bietet diese neue Technologie maximalen Schutz gegen die zunehmend raffinierter werdenden Bedrohungen und Angriffe.<br />IBM MobileFirst Protect Threat Management nutzt die flexiblen Möglichkeiten der Cloud und verknüpft sie mit effektiven Sicherheitsinstrumenten zur Bekämpfung von Missbrauch und Malware im Kontext von Enterprise Mobility Management.<br />Unter http://bit.ly/1DG5AtF kann IBM MobileFirst Protect Threat Management kostenlos getestet werden.<br />(1) Arxan Technologies: https://www.arxan.com/assets/1/7/Arxan_Application_Protection_with_IBM_Trusteer_-_Solution_Brief.pdf <br />(2) IBM X-Force Threat Intelligence Quarterly 1Q 2015: http://ibm.co/1wEMKV3 <br />Über IBM Security: <br />Das Security-Portfolio der IBM bietet intelligente Lösungen, um Mitarbeiter, Daten, Anwendungen und Infrastrukturen umfassend zu schützen. Dazu gehören Identitäts- und Zugangsmanagement, Informations- und Eventmanagement, Sicherheitslösungen für Datenbanken, Anwendungsentwicklung, Risiko- und Endpoint-Management, Intrusion Protection und vieles mehr. IBM ist einer der weltweit größten Entwickler und Anbieter von Sicherheitslösungen.<br />Mehr Informationen auf www.ibm.com/security , @IBMSecurity auf Twitter<br />Über IBM:<br />Mehr Informationen finden Sie unter http://www.ibm.com/de <br />Kontaktinformation<br /><br />Hans-Jürgen Rehm<br />Unternehmenskommunikation<br />IBM Deutschland<br />Smarter Computing, Security<br />+49 7034 15 1887<br />+49 171 556 69 40<br />hansrehm@de.ibm.com<br /><img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=590890" width="1" height="1">

### Pressekontakt

IBM Deutschland

71137 Ehningen

hansrehm@de.ibm.com

### Firmenkontakt

IBM Deutschland

71137 Ehningen

hansrehm@de.ibm.com

IBM gehört mit einem Umsatz von 95,8 Milliarden US-Dollar im Jahr 2009 zu den weltweit größten Anbietern im Bereich Informationstechnologie (Hardware, Software und Services) und B2B-Lösungen. Das Unternehmen beschäftigt derzeit 399.400 Mitarbeiter und ist in über 170 Ländern aktiv.Die IBM in Deutschland mit Hauptsitz bei Stuttgart ist die größte Ländergesellschaft in Europa.Mehr Informationen über IBM unter: ibm.com/de/ibm/unternehmen/index.htmlIBM ist heute das einzige Unternehmen in der IT-Branche, das seinen Kunden die komplette Produktpalette an fortschrittlicher Informationstechnologie anbietet: Von der Hardware, Software über Dienstleistungen und komplexen Anwendungslösungen bis hin zu Outsourcingprojekten und Weiterbildungsangeboten.