Mobile Security in Deutschland 2015

IDC Studie untersucht die Nutzung mobiler Geräte im Unternehmensumfeld

Wiesbaden, 11. August 2015 Die Bedrohungslage für die Unternehmens-IT bleibt durch immer neue mobile Geräte und Anwendungen durchgehend anspruchsvoll und dynamisch – hierauf müssen Unternehmen mit ihren Sicherheitssystemen reagieren. Das Marktforschungs- und Beratungsunternehmen IDC hat zusammen mit Sophos und anderen Unternehmen eine Studie zur mobilen Sicherheit im Unternehmensumfeld durchgeführt. Ziel der Befragung unter 243 IT-und Fachbereichs-Entscheidern aus Unternehmen in Deutschland mit mehr als 100 Mitarbeitern im Mai 2015 war es, ein besseres Verständnis für das Bedrohungspotenzial sowie die Anforderungen, Maßnahmen und Pläne zur Absicherung der mobilen Technologien in Organisationen zu gewinnen. Die Studie zeigt Trends und Entwicklungen in Deutschland auf und beleuchtet unter anderem etwa die aktuelle Bedrohungslage, den Einsatz verschiedener Lösungen wie Daten-Container oder auch besondere Aspekte, die sich aus Filesharing-Aktivitäten der Mitarbeiter und Wearables ergeben. Es werden zudem die Sicherheit mobiler Apps, Multifaktor-Authentifizierung, Biometrie und Sprachverschlüsselung beleuchtet.
Im Folgenden einige Ergebnisse der Studie:

Risikofaktor Mitarbeiter
Als größtes Sicherheitsrisiko schätzen die befragten IT-Verantwortlichen die Gefahr durch mobile Malware ein, deren Verbreitung auch in der heterogenen mobilen Betriebssystemlandschaft in den letzten Jahren deutlich zugenommen hat. Darüber hinaus zählen mehr als ein Drittel der Befragten Phishing-Attacken zu den drei größten Risiken. Als drittgrößte Gefahr identifizierten die Befragten die Anwender – also Mitarbeiter selbst. Ihr Fehlverhalten, sei es beabsichtigt oder versehentlich, fürchten 30 Prozent der befragten Entscheider. 43 Prozent der sicherheitsvorfälle gehen nach Ansicht der Entscheider auf das Konto von Mitarbeitern, 30 Prozent der Fachbereichsleiter hatten zudem in den vergangenen zwei Jahren den Verlust eines Smartphones in ihrem Fachbereich zu beklagen.

Verschlüsselt sprechen, unverschlüsselt senden
Im professionellen Umfeld ist es zunehmend Usus, vertrauliche Telefonate über das Smartphone zu verschlüsseln. Bereits ein Drittel der Befragten Unternehmen setzt zu diesem Zwecke eine App ein. Auch Messenger Dienste werden in steigendem Maße beruflich genutzt. Hier herrscht allerdings aus Sicht von IDC eine noch zu hohe Sorglosigkeit bei den befragten Unternehmen, was die Chat-Sicherheit von Diensten wie WhatsApp und Facebook angeht.

Training und Richtlinien und Training
Es reicht nicht aus, die IT-Verantwortlichen und Key-User in Unternehmen in Sachen Sicherheit zu schulen, gerade die Mitarbeiter – als Risikofaktor bekannt – müssen im Umgang mit Datensicherheit auf sämtlichen Geräten geschult werden. Mitarbeitertrainings sind aus Sicht der IT-Entscheider hierfür am besten geeignet. An zweiter Stelle folgt die Durchsetzung einer Mobile Security Policy und der Schulung des IT-Personals. Aus IDC-Sicht sollte eine Mobile-Security-Richtlinie nicht isoliert betrachtet, sondern vielmehr in das unternehmensweite IT-Sicherheitskonzept integriert werden. Sowohl Richtlinien sowie sich ergebende Konsequenzen aus deren Nichteinhaltung sollten den Mitarbeitern bewusst gemacht werden. Hierfür – wiederum – sind Schulungen und Trainings notwendig.

Container-Lösungen
Container-Lösungen ermöglichen es, mobile Applikationen und Dateien eines Unternehmens in einer geschützten Umgebung zu verwalten. Durch die Verwendung eines Containers auf einem mobilen Endgerät können außerdem die privaten von den geschäftlichen Informationen getrennt werden.
54 Prozent der befragten Unternehmen setzen heute bereits Container auf Smartphones und Tablet-PCs ein. Allerdings nannte nur ein Drittel dieser Organisationen die Trennung von privaten und geschäftlichen Inhalten als zentrales Ziel ihrer Lösung; 67 Prozent führten einen besseren Schutz für Firmendaten auf mobilen Geräten an.

Empfehlungen
IDC richtet auf Grundlage der Studienergebnisse einige Empfehlungen an die Unternehmen, darunter finden sich wichtige Punkte wie

- Betrachten Sie Mobile Security nicht isoliert, sondern als wichtigen Teil Ihres IT-Sicherheitskonzepts
- Sensibilisieren Sie Anwender für die Risiken im Umgang mit ihrer mobilen IT
- Verschaffen Sie sich Transparenz in einem unübersichtlichen Markt
- Setzen Sie sich mit den Auswirkungen von Wearables auf Ihre IT-Sicherheit auseinander

Praxisblick
In einem ergänzenden Interview äußert sich Sascha Pfeiffer, Principle Security Consultant bei Sophos, aus Praxisperspektive zu den Studienergebnissen. Die notwendige, gute Balance zwischen Produktivität und Sicherheit bewertet er beispielsweise so: „In der Praxis zeigt sich, dass Endnutzer durchaus bereit sind, ein bestimmtes Maß an Kontrolle über ihre mobilen Geräte abzugeben, um mehr Flexibilität, Effizienz und Produktivität zu gewinnen. Gleichzeitig benötigen IT-Abteilungen genug Kontrollmöglichkeiten, um BYOD-Programme optimal verwalten und für Sicherheit sorgen zu können. Ganz gleich, ob Unternehmen also ihren Mitarbeitern mobile Geräte zur Verfügung stellen oder ob diese ihre Privatgeräte mitbringen: der Überblick über alle Geräte im Netzwerk und der Daten darauf ist entscheidend.“

Den Executive Brief zur Studie lesen Sie hier:
https://www.sophos.com/de-de/security-news-trends/whitepapers.aspx

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos‘ Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.
Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-40-484434
sophos@tc-communications.de