# BETRIEBSGEHEIMNIS AUF DEM SMARTPHONE

*Belarussische Staatliche Universität für Informatik und Radioelektronik Minsk, Republik Belarus*

*Drozdovskiy N. S.*

*Matalyga S. A. – Dozentin des Lehrstuls №1*

In unserem zeit gibt es viele Spionage- oder Sabotagesoftware aber in bekannten Organizationen gibt es eigene Methode, um diesem Malwaresoftware zu wiederstehen.Diese Methoden werden in diesem Artikel erzählt.

Seit geraumer Zeit spukt ein technishes Schreckgespenst durch die IT-Abteilungen vieler Unternehmen. “Bring your own device”, kurz BYOD. Oder mit anderen Worten: die dienstliche Nutzung privater Technik durch Angestellte und Mitarbeiter. Das gilt zwar als praktish, preiswert und zeitgemäß. Doch es hat auch einen Haken: Die Sicherheit der firmeneigenen Datensysteme steht auf dem Spiel. Nach einer Umfrage des IT-Branchenverbandes Bitkom vezichtet fast die Hälfte aller Unternehmen auf Sicherheitregeln für Mobilgeräte. “Wir empfehlen den Unternehmen dringend, wirksame Regeln für Sicherheitsfragen einzufürhen”, erklärte Bernhard Rohleder, Hauptgeschäftsführer des Bitkom.

Das ist auch notwendig: Denn kaum noch ein Büro, in dem Beschäftigen nicht über die Bildschirme unt Tastaturen ihrer privaten Smartphones, Tablet- oder Laptopcomputer streichen, um innerbetriebliche E-Mails zu beantworten, um Excel-Tabellen zu erstellen oder um einen Geschäftsbrief zu schreiben. Denn private IT-Geräte sind oft leistungfähiger als die, die in der Firma stehen. Wurde die technishe Entwicklung in der IT-Industrie einst von schrankwandgroßen Zentralrechnern und vernetzten Personalcomputern (PC) gesteuert, so wird sie seit dem Aufkommen von internetfähigen Mobiltelefonen(Smartphones) und Tabletcomputern vor zehn Jahren von den Wünschen und Möglichkeiten einfacher Konsumenten vorangetrieben. Im Neudeutsch heißt das: “Die Consumerization der IT”. In der Arbeitswelt äußert sich das durch “Bring your own device”.

Diese sogenannte BYOD-Bewegnung bringt die neueste Technik zum Einsatz, lässt aber auch die Grenzen zwischen Berufs- und Privatleben verwischen. Das Internt verbindet. Denn jeder ist zu jeder Zeit an jedem Ort erreichbar. Dabei hat die Flut an kleinem tragbaren Hochleistungscomputern noch gar nicht ihren Höhepunkt erreicht. Im vergangenen Jahr wurden nach Angaben des Bitkom in Deutschland meht als 4,4 Millopnen Tabletcomputer und fast 22 Millionen Smartphones verkauft, doppelt so viel wie im Jahr zuvor. Ein Ende des Wachstums ist nicht in Sicht: Einer Erhebung des kalifornischen Netzwerkspezialisten Cisco zufolge hat heute jeder Beschäftigte in Deutschland im Durchschnitt 1,8 Computergeräte im Einsatz; in zwei Jahren sollen es 2,2 Geräte sein. Zwei Drittel der von Cisco befragten 5.000 IT-Manager bewerten die BYOD-Bewegung als positiv. Viele Firmenchefs erhoffen sich Produktivitätsigewinne und – zumindest langfristig – Einparpotential, weil die Beschäftigten mit den eigenen Geräten besser umgehen können als mit denen, die ihnen der Arbeitgeber bereitstellt. Doch jede Medaille hat zwei Seiten: Plus steht das Minus mangelnder Datensicherheit gegenüber. Etwa wenn Beschäftigte ihre privaten Mobilgeräte ins hausinterne Firmennetzwerk einloggen wollen und auf diese Weise, bewusst oder versehentlich, virenbehaftete Daten einschleusen, im Extremfall gar Sabotage- oder Spionagesoftware. Alles nur Panikmache? Kaum! Denn was geschieht, wenn private Geräte mir sensiblen Unternehmensdaten verlorengehen oder gestohlen werden? Wer haftet, wenn Kunden- oder Mitarbeiterdaten in die falschen Hände geraten? Und wie steht es um Datenschutz und Privatsphäre, wenn Geräte in zwei Welten eingesetzt werden?

“Wir haben heute über 20.000 iPads im Einsatz, Tendenz steigend”, sagt Oliver Bussmann, Chief Information Officer (CIO) von Europas größtem Softwarehaus SAP. Der IT-Konzern IBM beschäftigt fast eine halbe Million Mitarbeiter in aller Welt. 80.000 Angestellte nutzen auch während der Arbeit ihre eigenen privaten Smartphones und Computer. Jeanette Horan, CIO von IBM, erklärte in einem Interview, der Konzern habe schon vor Jahren eine “mobile Belegschaft” aufgebaut. Ausgagspunkt waren die ersten sogenannten E-Mail-Trackers der Marke Blackberry. Die waren kaum größer als ein Handy und kamen 1999 auf den Markt. Vier Jahre später war die Funktionalität erhöht und der Typenname Smartphone geprägt.

2007 stieg Apple in den Markt ein und brachte das erste Iphone heraus. 2010 folgte der Tabletcomputer iPad. Nach den Worten von SAP-CIO Bussmann habe das einen “enormen Schub gebracht”. Hasso Plattner, einer der fünf Gründer von SAP und heutiger Vorsitzender des Aufsichtsrats, war einer der Ersten, die ein iPad besaßen. Damals habe man erkannt, dass die Zukunft darin liegt, Unternehmensanwendungen auf mobile Geräte zu bringen, sagt Bussmannn. “Wir verwalten alle unsere mobilen Geräte mit der firmeneigenen Software SAP Afaria”, erklärt Bussmann. Durch ein sogenanntes “Enrollment” werde jedes Smartphone oder das Tablet in die “mobile Infrastruktur des Unternehmens eingebunden und auch abgesichert”. Somit habe die IT-Abteilung die Kontrolle über die Geräte. IBM geht ähnlich vor. Zwar werde jeder Mitarbeiter mit einem hauseigenen, IBM-sicherheitszertifizierten Notebook ausgestattet. Doch CIO Jeanette Horan ließ darüber hinaus auch die berufliche Nutzung privater Geräte zu. Dafür jedoch führte sie klare Spielregeln ein. So wird die hauseigene Anwendungs- und Sicherheitssoftware auf jedes dieser Privatgeräte aufgespielt, um sicher zu gehen, dass sich keine Sicherheitslücken im betrieblichen Einsatz auftun.

Der Quelle:

1. Goethe Institut. die Zeitschrift “MARKT Deutsch für den Beruf – Materialien aus der Presse