

Pressestatement

Prof. Dieter Kempf, Präsident BITKOM

Vortrag im Rahmen der Pressekonferenz mit dem BKA zu Cyberkriminalität

Berlin, 27. August 2014

Seite 1

Vielen Dank, lieber Herr Ziercke!

Sie haben gerade das große Dunkelfeld in der Statistik angesprochen. Neben den tatsächlich bei der Polizei angezeigten Fällen gewinnen wir mit unseren Umfragen wichtige Erkenntnisse zur Cyberkriminalität. Sie zeigen, wie stark die Nutzer von Computer und Internet von Systemausfällen, Datendiebstahl, Betrug oder sonstigen Delikten betroffen sind. Dazu haben wir auch in diesem Jahr wieder eine repräsentative Befragung unter 1.000 Internetnutzern durchgeführt.

Wovon fühlen sich die Menschen bedroht, wenn sie im Internet unterwegs sind?

Die größte Sorge bereitet, dass persönliche Daten ausspioniert werden. Vier von fünf Internetnutzern fürchten eine Ausspähung durch Staat, Kriminelle oder Unternehmen. Und zwar in dieser Reihenfolge. Die Angst vor der Bespitzelung durch den Staat ist heute größer als die Angst vor Cyber-Kriminellen. Das ist eine Folge der Abhöraktionen staatlicher Geheimdienste im Internet. An zweiter Stelle folgt bei zwei Dritteln (68 Prozent) die Angst vor der Infizierung des Computers mit Schadprogrammen wie Viren oder Trojanern. Ebenfalls weit verbreitet ist mit einem Anteil von 63 Prozent die Sorge vor Betrug im Rahmen von finanziellen Transaktionen wie Online-Shopping oder Online-Banking. Ein Viertel hat Angst vor Mobbing oder Belästigungen im Netz. Nur jeder Zehnte (11 Prozent) fühlt sich gar nicht bedroht. Zum Vergleich: Vor drei Jahren waren es noch 21 Prozent, die keinerlei Befürchtungen hatten.

Wir wollten nun wissen, wie die gefühlte Bedrohung mit den tatsächlichen Erfahrungen der Nutzer korrespondiert. 55 Prozent der Internetnutzer sind nach eigener Aussage in den vergangenen zwölf Monaten Opfer von Cyberkriminalität in der einen oder anderen Form geworden. Das entspricht rund 29 Millionen Betroffenen. Bei vier von zehn Internetnutzern wurden die Computer mit Schadprogrammen infiziert. Knapp ein Fünftel (19 Prozent) gibt an, dass Zugangsdaten zu Internetdiensten ausspioniert worden sind. 14 Prozent sind von einem Geschäftspartner betrogen worden, zum Beispiel beim Online-Shopping

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin
Tel. +49.30.27576-0
Fax +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Maurice Shahd
Pressesprecher
+49. 30. 27576-114
m.shahd@bitkom.org

Präsident

Prof. Dieter Kempf

Hauptgeschäftsführer

Dr. Bernhard Rohleder

Prof. Dieter Kempf, Präsident des BITKOM

Vortrag im Rahmen der Pressekonferenz mit dem BKA zu Cyberkriminalität

Seite 2

oder einer Auktion. Ein weiteres häufig genanntes Delikt (von 16 Prozent) ist der illegale Versand von E-Mails in fremdem Namen.

Der Mangel an Vertrauen und die Sorge vor Cyberkriminalität führen dazu, dass viele Verbraucher auf die Nutzung bestimmter Online-Dienste verzichten. 47 Prozent verschicken vertrauliche Dokumente nicht per E-Mail, fast ein Drittel (29 Prozent) verzichtet auf Online-Banking und ein Viertel (24 Prozent) auf das Einkaufen im Internet. Ebenfalls ein Viertel macht einen Bogen um soziale Netzwerke, ein Fünftel (21 Prozent) nutzt keine Cloud-Dienste und 17 Prozent buchen weder Reisen noch Mietwagen im Netz. Das sind alarmierende Zahlen, weil dieser Trend die digitale Entwicklung bremst. Allerdings zeigt der Vergleich mit dem Jahr 2011, dass die NSA-Affäre dafür nicht den Ausschlag gegeben hat. Es besteht bei vielen Menschen offenbar ein generelles Unbehagen, dass durch die Abhöraktionen Bestätigung gefunden hat.

Es gibt eine Reihe von Möglichkeiten, wie sich Internetnutzer schützen können. Gut ausgestattet sind die Nutzer mit Virenschutzprogrammen und Firewalls, die unberechtigte Zugriffe von außen auf den Computer verhindern. Neben den im Betriebssystem integrierten Schutzprogrammen haben viele Nutzer zusätzliche Sicherheitspakete installiert. Langsam aber sicher kommen Verschlüsselungssysteme aus der Nische, die den Zugriff auf persönliche Daten unterbinden. Immerhin 16 Prozent der Internetnutzer verschlüsseln E-Mails und 15 Prozent Dateien. 16 Prozent geben an, dass sie mit Anonymisierungsdiensten wie Tor im Internet surfen. Der Vergleich zum Vorjahr zeigt: Seit Juli 2013, als die Abhöraktionen ans Licht gekommen sind und wir das erstmalig abgefragt haben, ist die Nutzung von Verschlüsselungs- und Anonymisierungssystemen deutlich gestiegen.

Allerdings sind die technischen Hürden für die Verschlüsselung persönlicher Informationen immer noch sehr hoch. 61 Prozent derjenigen, die keine Verschlüsselung nutzen, geben als Begründung an, dass sie sich damit nicht auskennen. 54 Prozent nennen als Grund für ihren Verzicht, dass ihre Kommunikationspartner ebenfalls keine Verschlüsselung einsetzen. Und nur in diesen Fällen machen kryptografische Verfahren auch tatsächlich Sinn. Einem Drittel ist die Nutzung schlicht zu aufwändig.

Bequemlichkeit ist der größte Feind der IT-Sicherheit. In den vergangenen Monaten waren die Medien voll von Berichten über groß angelegte Hacker-Angriffe auf Online-Dienste, bei denen personenbezogene Daten von Hunderttausenden Kunden entwendet wurden. Damit einher ging die dringende Aufforderung an die

Prof. Dieter Kempf, Präsident des BITKOM

Vortrag im Rahmen der Pressekonferenz mit dem BKA zu Cyberkriminalität

Seite 3

User, ihre Passwörter zu ändern. Tatsächlich getan haben das laut unserer Umfrage immerhin 60 Prozent der Internetnutzer. Auf der anderen Seite hat mit 38 Prozent mehr als jeder Dritte keine Änderungen an seinen Passwörtern für E-Mail-Dienste, Shopping-Seiten, Online-Banking etc. vorgenommen. Diese Sorglosigkeit kann fatale Folgen haben, wenn Zugangsdaten missbraucht werden. Das gleiche gilt, wenn Internetnutzern grundlegende Verhaltensweisen unbekannt sind oder ignoriert werden. Dazu gehört zum Beispiel, keine Anhänge oder Links in E-Mails unbekannter Absender zu öffnen.

Zunehmend im Fokus steht das Problem der Wirtschaftsspionage. Alle wichtigen Geschäftsgeheimnisse eines Unternehmens liegen heute in digitalisierter Form vor. Dabei ist es unerheblich, ob sensible Daten von staatlichen Geheimdiensten oder kriminellen Hackern gestohlen werden. Insbesondere der hoch spezialisierte deutsche Mittelstand mit seinen vielen hidden champions in den Bereichen Maschinenbau, Elektrotechnik oder Fahrzeugbau ist ein beliebtes Angriffsziel.

Nach unserer letzten Umfrage vom Jahresanfang gab es bei 30 Prozent der Unternehmen ab 20 Mitarbeitern in den vergangenen zwei Jahren IT-Sicherheitsvorfälle. Die Befragung bestätigt, dass die kleineren und mittleren Unternehmen mit 20 bis 499 Mitarbeitern mit einem Anteil von 31 Prozent deutlich stärker betroffen sind. Bei den großen Unternehmen ab 500 Mitarbeitern verzeichneten nur 11 Prozent IT-Sicherheitsvorfälle in den letzten zwei Jahren. Auch hier gibt es ein großes Dunkelfeld, da viele Angriffe unentdeckt bleiben.

Die meisten IT-Sicherheitsvorfälle werden „vor Ort“ verursacht. 58 Prozent der attackierten Unternehmen sagen, dass die Störungen von eigenen oder externen Mitarbeitern verursacht wurden. In der Regel kennen sich diese so genannten Innentäter mit den Gegebenheiten in den Betrieben gut aus und stehlen gezielt bestimmte Datensätze oder schleusen Schadprogramme in die IT-Systeme ein. Eine andere Methode besteht darin, Mitarbeitern mit Computer-Viren verseuchte USB-Sticks unterzuschieben. Oder sie werden von Kriminellen dazu verleitet, Informationen preiszugeben. Im Fachjargon sprechen wir von Social Engineering. Darüber hinaus berichtet fast ein Drittel (30 Prozent) der Unternehmen, dass Angriffe auf die IT-Systeme über das Internet erfolgt sind. Hierzu zählen Denial-of-Service-Attacken oder gezielte Einbrüche in die IT-Systeme über das Internet.

Chart: Gut ein Drittel verstärkt IT-Sicherheit infolge der NSA-Affäre

Prof. Dieter Kempf, Präsident des BITKOM

Vortrag im Rahmen der Pressekonferenz mit dem BKA zu Cyberkriminalität

Seite 4

Nach unserer Erfahrung ist das Bewusstsein für das Thema IT-Sicherheit insbesondere bei kleineren und mittleren Unternehmen noch zu gering ausgeprägt. Nach der NSA-Affäre, die als Weckruf in Sachen IT-Sicherheit gilt, haben nur gut ein Drittel (36 Prozent) der befragten Unternehmen ihre IT-Sicherheitsmaßnahmen verstärkt. Knapp ein Viertel (23 Prozent) hat die Ausgaben zum Schutz der IT-Systeme erhöht. Das reicht aus unserer Sicht nicht aus. Alle Unternehmen sollten regelmäßig ihre IT-Sicherheitsarchitektur sowohl in technischer als auch organisatorischer Hinsicht überprüfen.

Ich fasse zusammen: die Computerkriminalität ist insgesamt nicht dramatisch angestiegen. Es gibt keinen Grund zur Panik. Sie ist aber – wie viele andere Delikte aus der nicht-digitalen Welt – inzwischen allgegenwärtig. Die Sicherheit informationstechnischer Systeme ist daher längst kein Thema für IT-Nerds mehr, sondern sie ist für die gesamte Gesellschaft relevant. Die Mehrheit der Bevölkerung benutzt Computer, Internet, Smartphones etc. Mit der zunehmenden Vernetzung von Fernsehern, Haushaltstechnik oder Fahrzeugen ergeben sich neue Risiken. Gleichzeitig besteht die Gefahr, dass über digitale Wirtschaftsspionage wichtiges Know-how aus Deutschland abfließt. Darüber müssen wir die Anwender aufklären. Das setzt aber die Bereitschaft voraus, sich mit dem Thema zu beschäftigen. Wie Teilnehmer im Straßenverkehr müssen sich Internetnutzer im Web auskennen, die Regeln beachten und ein Gefühl dafür entwickeln, wo Gefahren lauern und welche Risiken von Ihnen ausgehen können. Eine zentrale Rolle auf diesem Weg spielen Initiativen, die sich intensiv um die Information der Internetnutzer bemühen. Wir machen als BITKOM selbst vieles, zum Beispiel als Mitglied der Initiative Deutschland sicher in Netz. Das BKA oder das Bundesamt für Sicherheit in der Informationstechnik halten ebenfalls umfangreiche Informationen bereit. Diese Initiativen müssen wir ausbauen und stärker koordinieren. Die IT-Branche wird in jedem Fall alles daran setzen, durch noch bessere Produkte und Dienste, aber auch durch eine bessere Information der Verbraucher die Sicherheit im Internet zu erhöhen.

Vielen Dank!