BEILAGE ZUM DSD 4 | 2016

BDSW

INFO
WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

Wozu in die Ferne schweifen...

WOZU IN DIE FERNE SCHWEIFEN, WENN DAS SCHLECHTE LIEGT SO NAH. Dieses leicht umgewandelte geflügelte Wort des Dichterfürsten Johann Wolfgang von Goethe gewinnt eine besondere und höchst aktuelle Bedeutung, wenn es um die Abhörsicherheit von Mobiltelefonen geht.

Ja, wozu eigentlich in die Ferne schweifen... Wir haben in den zurückliegenden Monaten unendlich viel über Lauschangriffe von ausländischen Nachrichtendiensten, namentlich der NSA, gelesen. Medienberichte über belauschte Handys – Stichwort Merkelphone – gab es en masse. Wenig berücksichtigt wurde dabei allerdings, dass es keinesfalls der immensen technischen Möglichkeiten großer Nachrichtendienste bedarf, um ein x-beliebiges Mobiltelefon anzuzapfen. Ein Spionagetool, das zwischen 100 und 150 Euro Jahresgebühr kostet, genügt – und schon kann jeder, der will, problemlos mithören. Einzige Voraussetzung: Der Lauscher in spe muss ein paar Minuten Zugang zum jeweiligen Handy oder Smartphone haben. Danach reicht ein Internetzugang und ein handelsüblicher PC, um den Angriff zu starten.

Das ist leider keine überbordende Fantasie, sondern betrübliche Realität. Wer die so genannte Tracking-Software, bezeichnende Handelsnamen sind mSpy oder FlexiSpy, erwerben will, muss nicht etwa in die düstere Welt des Darknets eintauchen. Es genügt völlig, das ganz normale Internet zu besuchen. Denn der Verkauf der Spionageprogramme ist legal. Auch die Benutzung ist es – solange die Schnüffel-Software auf das eigene Mobiltelefon geladen wird.

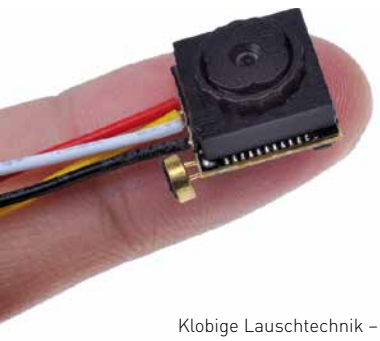
Das unberechtigte Aufspielen auf fremde Handys / Smartphones erfüllt allerdings gleich mehrere Straftatbestände. Wer andere Geräte mit den Spionageprogrammen infiziert, verstößt unter anderem gegen Art. 10 des Grundgesetzes (Fernmeldegeheimnis) und die Vertraulichkeit des nicht öffentlich gesprochenen Wortes, § 201 StGB. Beide sind alles andere als Kavaliersdelikte. Doch ohnehin Kriminelle dürfte das kaum abschrecken.

Wir müssen ohne falschen Alarmismus zumindest im Hinterkopf behalten, dass ein Lauschangriff theoretisch jederzeit möglich ist. Denn besser und billiger als durch ein Spionageprogramm kommt niemand an sensible Informationen und Betriebsgeheimnisse heran. Inklusive Details aus unserer Privatsphäre, die aus gutem Grund keinen Außenstehenden etwas angehen und deren unbefugte Kenntnis nicht nur für uns selbst, sondern auch für unsere Familien eine akute Gefahr darstellen kann.

Ein auch nur einige Minuten unbeaufsichtigtes Mobiltelefon ist ein Sicherheitsrisiko ersten Ranges. Ein wenig wohlmeinendes Gegenüber könnte sich allein durch Lesen der Kontaktliste oder der zuletzt gewählten Nummern ein Bild über Sie machen. Oder – noch folgenreicher – ein Spionageprogramm auf das Handy oder Smartphone downloaden. Was passiert, wenn Letzteres realisiert wird, ist unglaublich. Das Mobiltelefon wird zur Superwanze, die unsere Bewegungen überwacht und alles preisgibt, was mit dem Handy oder Smartphone veranstaltet wird – und das ist im Zeitalter der Technik viel, sehr viel. Details ersehen Sie aus unserem nächsten Beitrag.

Was wir empfehlen: Hüten Sie Ihr Mobiltelefon wie Ihren Augapfel. Anders ist es nicht zu verhindern, dass Sie möglicherweise mit einer Wanze herumlaufen, die mehr von Ihnen und Ihrem Unternehmen preisgibt, als es auch der fähigste Spion vermag.

Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz



Klobige Lauschtechnik – das war einmal. Diese fingerspitzengroße „Lochcam" kann nicht nur Bilder, sondern auch sämtliche Umgebungsgeräusche übertragen. Foto: ArchivG

Herumliegende Mobiltelefone und andere Highlights für Eindringlinge

Von Klaus Henning Glitza

EINER PERSON, DER ES GELINGT, IN IHR UNTERNEHMEN EINZUDRINGEN, ERÖFFNEN SICH WAHRHAFT FANTASTISCHE MÖGLICHKEITEN DER SPIONAGE. Wir haben diese Thematik bereits in der vorigen Ausgabe von „Info Wirtschaftsschutz" angerissen und setzen sie heute aus gegebenen Anlässen fort. Denn es ist ein Faktum, dass auch in den Zeiten von Hightech der illegale direkte Zugang viele Angriffsformen erst möglich macht. Ein Beleg dafür, dass klassischer Wachschutz und physische Sicherheit keinesfalls zum „alten Eisen" gehören, sondern auch heute noch Grundlage jedes wirksamen Know-how-Schutzes sind. Genauso falsch, wie den alleinigen Schwerpunkt auf physische Sicherheit zu legen und die IT-Sicherheit zu vernachlässigen, ist der umgekehrte Ansatz. Angreifer am unerwünschten physischen Zugang zu hindern, ist deshalb unverzichtbar für jede Art von Unternehmenssicherheit, die diesen Namen verdient.

Ein Highlight für Eindringlinge, aber auch für Innentäter, sind nicht nur IT-Geräte, sondern auch internetfähige Mobiltelefone, die unbeaufsichtigt herumliegen. Das ist erstaunlich oft der Fall, wie jeder von uns, der mit offenen Augen durch die Welt geht, unschwer selbst feststellen kann. Denn Hand aufs Herz: Wer lässt sein Handy oder Smartphone nicht irgendwann aus den Augen. Ein paar Minuten der Abwesenheit, um Sanitärbereiche aufzusuchen, sich Kaffee zu holen oder kurz einmal zum Kopierer zu gehen, wäre es da nicht die reinste Form der Paranoia, das Mobiltelefon jedes Mal mitzunehmen?

Doch just diese paar Minuten genügen, um eine frei verkäufliche Spionagesoftware aufzuspielen, die zu den tückischsten Tools aller Zeiten gehört. Mit wenigen Handgriffen kann ein Mobiltelefon von einem Gerät, das seinem Nutzer gehorcht, zu einem ferngesteuerten Zombie, über den Dritte die volle Kontrolle haben, verwandelt werden. In Minutenschnelle kann ein nützlicher Helfer zu einem Spionagetool, wie es feindlicher kaum sein kann, umfunktioniert werden.

Eine Übertreibung? Wohl kaum! Was geschieht, wenn ein Spionageprogramm aufgespielt wird, ist zwar schier unglaublich, aber dennoch uneingeschränkt wahr. So kann mit einem „stillen" SMS-Befehl das infizierte Mobiltelefon jederzeit in eine Abhörwanze verwandelt werden. Still bedeutet, es wird eine Verbindung zum Handy / Smartphone aufgebaut, ohne dass es klingelt oder das Display aktiviert wird. Alles, was in der Nähe des Mobiltelefons gesprochen wird, kann dann mitgehört werden. Auch jene Kommunikation, die allein mit dem menschlichen Ohr kaum hörbar ist, kann ausgewertet werden. Professionelle Angreifer verfügen über technische Lösungen, um auch leiseste akustische Signale und Hintergrundgeräusche zu verstärken.

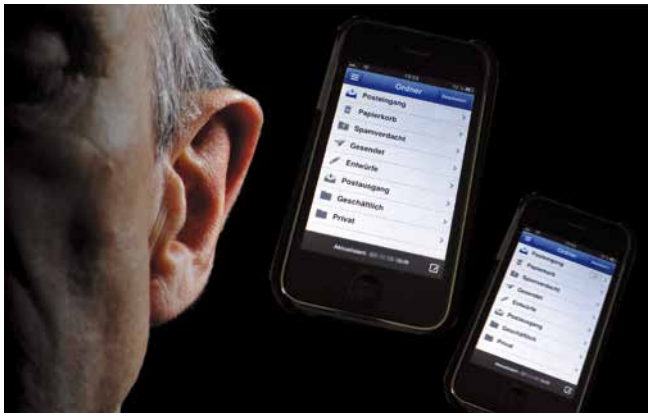
Abhören funktioniert auch ohne Funktechnik. Ein Aufzeichnungsgerät wie dieses kann irgendwo „vergessen" werden. Die fast schon standardmäßige Voice-Control-Funktionalität ermöglicht tagelanges Belauschen.
Foto: Tim Reckmann/pixelio.de

Zudem kann alles, was von dem Mobiltelefon übertragen oder empfangen wird, mitgehört beziehungsweise mitgelesen werden. Telefonate ebenso wie SMS, E-Mails oder Kommunikation über Skype und WhatsApp und ähnliche Dienste. Darüber hinaus wird jeder Internetzugang samt den Adressen der aufgerufenen Seite dokumentiert. Die Angreifer erhalten dadurch ein perfektes Bild über das Surfverhalten der Zielperson. Und natürlich lässt sich über die GPS-Funktionalität ein lückenloses Bewegungsprofil des Angegriffenen erstellen. Kurzum: Alles, was mit dem Handy getan wird, kann analysiert werden, wie Prof. Dr. Norbert Pohlmann, Leiter des Instituts für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen, deutlich macht.

Derart Angegriffene merken auf den ersten Blick nichts von diesen bösartigen Mutationen. Denn der professionelle Täter wird tunlichst alle Daten, die auf den irregulären Internetbesuch und den Download hinweisen, löschen. Alles scheint unverändert, ganz wie gewohnt.

Fatal: Die Mobiltelefone auszuschalten, ist entgegen landläufigen Meinungen kein wirksamer Schutz gegen mögliche Lauschangriffe. Selbst ausgeschaltete Geräte können zum Spionagetool werden. Die Spähprogramme ermöglichen es, heruntergefahrene Geräte unbemerkt wieder zu aktivieren, um sie als Wanze zu benutzen.

Zu entdecken ist die Schnüffelsoftware nur, wenn man genau darauf achtet. Denn auch die Hightech der Handyspionage hat eine Achillesverse: sie benötigt eine Internetverbindung, um die Audiodateien oder GPS-Positionsmeldungen zu über-



Wirtschaftlicher Feind hört mit: Handyspionageprogramme erlauben es, alles, was mit dem Mobiltelefon unternommen wird, 1:1 zu belauschen.
Foto: Bernd Kasper/pixelio.de

Überall dabei - das Mobiltelefon. Mit einem Spionageprogramm infiziert, wird es zur perfekten Abhörwanze, die auch ein lückenloses Bewegungsprofil erstellt. Selbst ausgeschaltete Handys/Smartphones können von Angreifern unbemerkt wieder aktiviert werden.
Foto: Bay. Landesamt für Verfassungsschutz

tragen. Früher wäre eine überdurchschnittliche Internetnutzung anhand der entsprechenden Rechnungspositionen aufgefallen, doch in den heutigen Zeiten der Datenflatrates scheidet diese Möglichkeit aus. Sie sollten also nach jedem Telefonat darauf achten, ob Ihr Handy / Smartphone online geht, ohne dass Sie dies selbst veranlasst haben. Ein Indiz ist auch, wenn der Akku sehr viel schneller in die Knie geht, als das vorher Fall war, ohne dass Sie selbst irgendetwas anders machen. Das kann zwar auch andere Ursachen haben wie die Überalterung des Akkus, doch ein Warnzeichen ist immer, dass die Schwäche des Energiespenders abrupt auftritt und nicht nach und nach.

Eine weitere Möglichkeit ist es, einen speziellen Virenscanner für Mobiltelefone zu nutzen. Doch achten Sie darauf, dass es der richtige ist. Das derzeit einzige Antivirenprogramm, das Spionagetools als schädliche Malware erkennt, ist F-Secure Mobile Anti-Virus. Sie können sich unter **http://mobile.f-secure.de** eine kostenlose, 30 Tage gültige Testversion direkt auf Ihr Mobiltelefon laden. Alternativ können Sie den Scanner mithilfe Ihres PC per Datenkabel oder Bluetooth downloaden. Ist das Herunterladen abgeschlossen, setzen Sie über „Optionen" die Funktion „Alles scannen" in Gang. Bei Funden wählen Sie die Menüpunkte „Details" und anschließend „Prozess". Dann können Sie eventuell vorhandene Malware per Knopfdruck löschen.

Mobiltelefone können aber auch in anderer Hinsicht eine Gefahr darstellen. Ein Besucher oder Innentäter könnte in Ihrem Büro ein Mobiltelefon „vergessen". Vorher hat diese Person die Nummer eines anderen Handys oder einer Festnetzverbindung gewählt. Über diese Dauerverbindung wird dann mitgehört, was der Besuchte sagt, nachdem sein Gast gegangen ist. In einem großen Land jenseits des großen Teichs ist dies eine bewährte Methode von Verkäufern, nach dem Verlassen eines Raums die möglichen Gegenargumente ihrer Gesprächspartner zu belauschen, um so ein Angebot machen zu können, das wie die Faust aufs Auge passt. Ein paar einfache Manipulationen, beispielsweise ein „totgeschaltetes" Display, verhindern, dass Zielpersonen den Sendebetrieb erkennen. Es gibt aber auch bei Spezialversendern Mobiltelefone, die speziell für solche Zwecke modifiziert sind.

Natürlich kann auch in solchen Fällen die bereits oben erwähnte Spionagesoftware ins Spiel kommen. Wir erinnern uns: das Mobiltelefon kann von einem beliebigen Gerät angerufen werden, ohne dass es klingelt. Der Einsatz des so genannten Tracking Tools auf dem eigenen Gerät ist noch nicht einmal strafbar. Allenfalls das Belauschen Dritter könnte strafrechtlich relevant sein. Sofern es beweiskräftig nachgewiesen werden kann, was nicht immer einfach ist.

Eine andere Möglichkeit ist ein analoges oder digitales Aufzeichnungsgerät, das z. B. einfach auf einen Schrank gelegt wird. Die heute gebräuchlichen Geräte sind fast ausschließlich mit einer Voice-Control-Funktion ausgestattet. Dadurch nehmen sie nur auf, wenn etwas gesprochen wird, und schalten in einen Standby-Modus, sobald Ruhe herrscht. Das spart Strom und verlängert die Aufnahmekapazität.

Es muss also nicht immer ein klassischer Miniatursender sein. Obwohl die Gefahr, dass Ihnen eine Wanze untergejubelt wird, nicht zu verkennen ist. Die heute gebräuchlichen Modelle haben mit den klobigen Vorgängerversionen, die noch vor zehn Jahren üblich waren, kaum noch etwas zu tun. Moderne Miniatursender sind so klein, dass sie in einem kleinen Stück Pappe Platz finden. Unter ein Tischbein geschoben, wirken sie wie ein harmloses Hilfsmittel, um ein Wackeln des Möbelstücks zu verhindern.

Und: Miniatursender waren niemals so schwierig zu detektieren wie heute. Das Scannen von Funkfrequenzen, eine früher gebräuchliche Methode, läuft heute ins Leere, weil es längst Abhörwanzen gibt, die nur kurzzeitig senden. Vorzugsweise zu nachtschlafenden Zeiten gibt der Miniatursender ein Signal von noch nicht einmal einer Sekunde ab, das stark komprimiert die gesamten, im Laufe des Tages gewonnenen Audiodaten übermittelt. Und das vorzugsweise per Satellitenfunk, was nochmals die Detektion erschwert. Neuere Miniatursender kommen außerdem ohne detektierbare Halbleiter aus. Ein weiteres Hemmnis für Lauschabwehrprüfungen, die sogenannten Sweeps. Moderne Wanzen sind zudem fernkonfigurierbar, das heißt, sie können einfach abgeschaltet werden, sobald es Anzeichen einer Prüfung gibt.

Das belegt abermals und kann gar nicht oft genug wiederholt werden: Physische Sicherheit ist das A und O jeder Sicherheit. Schützen und präventiv tätig zu werden, ist einfacher, als bereits realisierten Angriffen entgegenzuwirken.

BDSW/BfV Wirtschaftsschutztreff auf der security

IM RAHMEN DER WIRTSCHAFTSSCHUTZKOOPERATION zwischen BDSW und Bundesamt für Verfassungsschutz (BfV) fand am 28. September 2016 erstmalig auf der security in Essen am BDSW-Messestand ein gemeinsamer Wirtschaftsschutztreff von Unternehmens-, Behörden- und Verbandsvertretern statt. Teilnehmer waren seitens des Inlandsnachrichtendienstes BfV u. a. der Abteilungsleiter Spionageabwehr, Dr. Burkhard Even, sowie der Referatsleiter Wirtschaftsschutz, Bodo Becker. Der BDSW war u. a. mit dem Vizepräsidenten Peter H. Bachus; dem stv. Vorsitzenden des Arbeitskreises Wirtschaftsschutz Ralf Schuster; dem Hauptgeschäftsführer Dr. Harald Olschok, sowie dem Hauptstadtbüroleiter Dr. Berthold Stoppelkamp vertreten.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Dr. Berthold Stoppelkamp
Leiter des Hauptstadtbüros des BDSW und zuständiges Geschäftsführungsmitglied für den Arbeitskreis Wirtschaftsschutz

KPMG-Studie: Wirtschaftskriminalität in Deutschland 2016
BKA-Bundeslagebild Organisierte Kriminalität (OK)

Im Jahr 2015 führten die Strafverfolgungsbehörden in Deutschland 566 OK-Ermittlungsverfahren (2014: 571). In 36 Prozent der Verfahren geht es um Rauschgiftkriminalität, Eigentums- (14,8 Prozent) und Wirtschaftskriminalität (11,8 Prozent). Rund zwei Drittel der Tatverdächtigen sind ausländische Staatsangehörige. **www.bka.de**

BSI: Entwurf eines neuen Risikomanagement-Standards

Das BSI hat einen neuen BSI-Standard vorgestellt, der aus dem Modernisierungsprozess des IT-Grundschutzes hervorgegangen ist. In dem neuen Risikomanagement-Standard 200-3 sind erstmals alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes gebündelt in einem Dokument dargestellt.
www.bsi.bund.de

Bitkom-Studienbericht zum Wirtschaftsschutz in der Industrie

Im Rahmen einer repräsentativen Umfrage im Auftrag von Bitkom wurden 504 Unternehmen des produzierenden Gewerbes ab zehn Mitarbeitern befragt. Zu dem bereits im April 2016 vorgestellten Zahlenmaterial wurde nun ein ausführlicher Studienbericht unter Einbeziehung und Kommentierung von Experten veröffentlicht. **www.bitkom.org**

DSiN-Sicherheitsmonitor 2016

Nach wie vor wird in deutschen Unternehmen der Schutz gegen Cyberangriffe vernachlässigt. Zwar definiert zwischenzeitlich jedes vierte Unternehmen unternehmenseigene Schutzziele für die IT (2014: 21 Prozent), aber bei der Sensibilisierung von Mitarbeitern ist weiterhin nur jedes vierte Unternehmen aktiv (27 Prozent). Nur jedes dritte Unternehmen verfügt über einen Notfallplan. **www.sicher-im-netz.de**

BDSW

BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

Verantwortlich: Dr. Berthold Stoppelkamp
Redaktion: Henning Glitza

Norsk-Data-Straße 3 · 61352 Bad Homburg
Fon: +49 6172 948050 · Fax: +49 6172 458580

Mail: mail@bdsw.de
Web: www.bdsw.de