

Erstellt am: 10. 11. 2011 - 06:00 Uhr

## Abwehramt: "Unser Motto: Wissen schützt"

Oberst Walter Unger, IT-Security-Chef der Abwehr über Österreichs Nachholbedarf bei Internet-Sicherheit und den aktuellen Spionagefall gegen UN-Organisationen mit dem "Duqu"-Trojaner. Man ist "nicht überrascht".



Walter Unger, Leitung der Abteilung IKT-Sicherheit im Heeresabwehramt

"Vor zehn Jahren haben wir mit 40 Zuhörern begonnen", sodann sei die interne, jährliche Konferenz im Abwehramt sukzessive geöffnet und um Behörden, Firmen und Forscher erweitert worden, sagte Walter Unger, Leitung der Abteilung IKT-Sicherheit im Heeresabwehramt zu ORF.at.

Zu den insgesamt sechs Veranstaltungen 2011 würden 1000 Besucher erwartet, so Unger weiter, der sein Auge wohlgefällig auf den ersten Hundertschaften, die am Mittwoch eingetroffen waren, ruhen ließ.

### Live-Hacks von Handys

Am ersten Tag der zweitägigen Konferenz im Wiener Austria-Center war der große Saal voll besucht, als Marco Di Filippo vom Schweizer Unternehmen Compass Live-Hacks auf Mobiltelefonen demonstrierte.

Nach einem Parforceritt durch die Geschichte der Angriffe auf Telefonnetze schaffte es Di Filippo, in 50 Minuten Vortrag ein halbes Dutzend Live-Demos unterzubringen.

### Orten leicht gemacht

Von einfacher Selbstortung über die Lokalisierung anderer Handys mit einfachsten Methoden bis zum Abfangen eines Livegesprächs mit einem Teilnehmer aus dem Publikum reichte die Palette dieses obendrein in sehr launigem Ton gehaltenen Vortrags.

Beim Referat des Security- und Starkstromspezialisten Franz Lehner (Ikarus) über Angriffsvektoren auf das geplante System der intelligenten Stromzähler gab es dann weit weniger bis nichts zu lachen. Titel: "Smart Meters - Riskieren wir unsere Versorgungssicherheit?"

### "Smart Meters", Kopfschütteln

Zur Umsetzung der Verordnung der Regulationsbehörde E-Control müssen die Stromversorger eigene Kommunikationsnetze bis zu den Zählern einrichten, die mit den SAP-Systemen zur Kundenverwaltung verbunden werden.

Da die neuen "Smart Meters" auch Abschaltrelais enthalten, müssen die Steuersysteme der Stromnetze auf irgendeine Weise damit verbunden werden. Damit sind notwendigerweise wiederum die Kraftwerke vernetzt. Das halten Experten wie Lehner, oder Paul Karrer (Cyberscurity Austria), der ebenfalls vortrug, für potenziell gefährlich.

Danach: Kopfschütteln vor allem bei den zahlreich vertretenen Militärs. Bereits 2009 hatten denn auch Offiziere als erste Skepsis gegenüber der Art und Weise der geplanten Vernetzung geäußert. Tenor: angreifbar.

## **"Unser Motto: Wissen schützt"**

Was für ein möglicher Sicherheitsgewinn kann dann durch eine solche Veranstaltung erreicht werden?

Unger: "Unser Motto ist: Wissen schützt. Daher ist es unsere Aufgabe, dieses Wissen zu vermitteln und das auch so plakativ, wie in diesem Vortrag zur Handysicherheit." Allein, wenn einem in Sachen Security noch weniger Bewanderten dadurch bewusst werde, dass Nachholbedarf dringend gegeben sei, habe man das erste Ziel bereits erreicht, sagte der Oberst aus dem Abwehramt.

## **"Partikularinteressen? Nein, danke"**

Das zweite Ziel der Veranstaltung sei natürlich, Fachleuten eine Plattform zum Wissensaustausch zu bieten. Rund um die Seminare seien neuartige Kooperationen zwischen Behörden, Wirtschaft, aber auch Vereinen entstanden. Kooperationen, in denen eben auf Partikularinteressen keine Rücksichten genommen würden.

"Durch die allgegenwärtige, dichte Vernetzung sind auch neue Abhängigkeiten entstanden - ohne dass uns das tagtäglich bewusst ist. Sicherheit muss in diesem Zusammenhang umfassend und über Organisationsgrenzen gedacht werden", sagte der Oberst.

## **Angriff auf die UNO**

Wenige hundert Meter vor dem Austria Center erhebt sich das mächtige Rund der UNO-City. Das aktuelle Topthema in puncto IT-Sicherheit ist der "Duqu"-Trojaner, eine ebenso raffiniert wie aufwendig produzierte Schadsoftware-Kombination.

Sechs Organisationen oder Teile davon wurden in acht Ländern mit dieser von staatlichen Stellen Schadsoftware ausspioniert. Namen wurden von den damit befassten Antivirus-Herstellern natürlich nicht genannt.

Die Attacke richtete sich (auch) gegen Teilorganisationen der UNO. Die Aufstellung des Antivirushauses-Symantec listet unter den wenigen Fundorten des bis jetzt äußerst gering verbreiteten Duqu-Trojaners auch eine in einem österreichischen Netz. Es sind nicht mehr als ein Dutzend Fundorte in mutmaßlichen Zielnetzen bisher nachgewiesen. Die jedoch sind hochkarätig.

Rund um die Welt wird mit Hochdruck an der Analyse der ebenso raffinierten, wie rätselhaften Spionagesoftware "Duqu" gearbeitet. Sicher ist: Die Entwicklung der Schadsoftware hat mehrere Hunderttausend Dollar gekostet.

## **Das Abwehramt sagt**

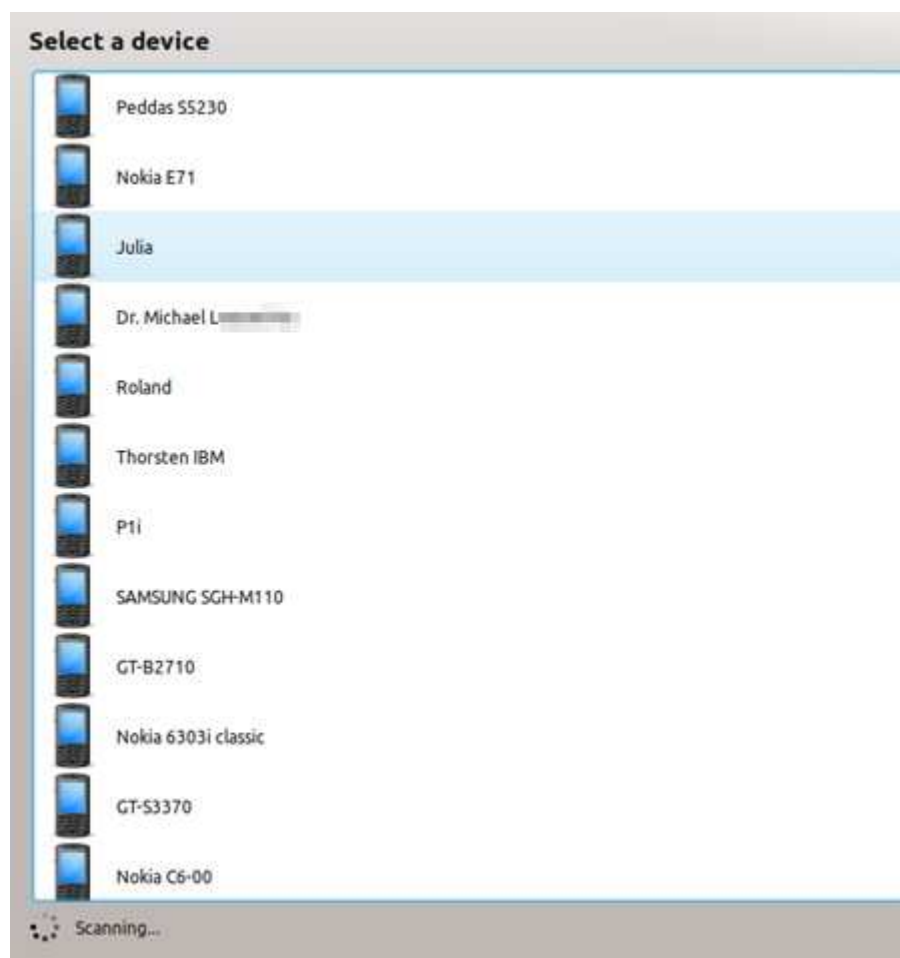
Der IKT-Sicherheitsschef des Heeresabwehramts müsste als solcher darüber eigentlich näher Bescheid wissen. Daher die Frage: "Können Sie das bestätigen?"

An diesem Punkt des Gesprächs umkam ein feines Lächeln des Obersts Züge. "Es sind in den letzten Jahren immer wieder großangelegte Spionageangriffe mittels Trojanern praktiziert worden. Auch internationale Behörden waren betroffen. Nicht alles wurde jedoch publiziert. Dass da nunmehr UNO-Organisationen durch Duqu betroffen sein sollen, verwundert mich daher überhaupt nicht."

## Bluetooth

Was den angesprochenen Nachholbedarf in Sachen Sicherheit angeht, so ließ sich der mit einem Bluetooth-Scan im Saal umgehend nachweisen. Beim kurzweiligen Vortrag Di Philippos "Sprach- und Datenspionage an Mobiltelefonen leicht gemacht", waren bei 24 Handys im Saal Bluetooth-Schnittstellen offen.

Eine posaunte sogar den vollen Namen samt akademischem Titel seines Besitzers in den Saal.



Das IKT-Sicherheitsseminar des Heeresabwehramts geht am Donnerstag Nachmittag zu Ende. Für Freitag ist - koordiniert vom Bundeskanzleramt - das erste österreichweite Treffen der Computer Emergency Response Teams von Behörden, Militärs und Organisationen aus dem Zivilbereich angesagt.