

# Computerworld

Nr. 46/2007 16. November Fr. 5.80 / € 3.90



## Fokus: Security

**Handy-Viren:** Die Gefahr steigt.

**Zero-Minute-Attacke:** Wie Sie Ihr Unternehmen schützen.

**Web-Bedrohungen:** Sieben gute Tipps für sicheres Surfen.

**Sterbehilfe:** Selbstzerstörung für geklaute Notebooks.

**EV-SSL:** Was bringt das neue Zertifikat gegen Phishing? **S. 14**

## Exklusiv-Interview

Warum ist BT in der Schweiz so erfolgreich? Country Manager Adrian Schlund packt aus. **S. 9**

## Weg mit der Röhre!

Die neuen Flachbildschirme mit 17, 19 und 20 Zoll. **S. 28**



## Windows Server 2008

Wie gut ist Microsofts neues Server-Betriebssystem? **S. 30**

**Pascal Lamia, IT-Securitybeauftragter des Bundes**

# Security: Messen, wie Mitarbeiter handeln

Die wegweisende «Twisk»-Methode macht endlich messbar, wie Mitarbeiter mit IT-Security umgehen. So wird es möglich, gezielt Abhilfe zu schaffen. **S. 12**



Pascal Lamia (links) und Daniel Graf, IT-Security-Beauftragte des Bundes, haben ermittelt, wie genau es die Beamten mit der IT-Sicherheit nehmen

# Security-Awareness wird messbar

Wie gehen Mitarbeiter mit der IT-Sicherheit um? Diese Frage wurde in der Bundesverwaltung untersucht. Dabei verhalf die wegweisende «Twisk»-Methode zu klar quantifizierbaren Ergebnissen, die jetzt in gezielte Awareness-Kampagnen münden. VON JENS STARK

**B**undesrats-Laptop weg! Als Bundesrätin Doris Leuthard ihre Tasche samt des darin verpackten Notebooks gestohlen wurde, schlugen die Wellen hoch. Die fetten Schlagzeilen sorgten für tiefe Kratzer im Security-Image der Bundesverwaltung. So etwas darf einfach nicht passieren. Trotzdem habe der Laptop-Klau auch etwas Gutes gehabt, denn er habe die Sensibilität der Bundesmitarbeiter für IT-Security markant geschärft, erklärt Pascal Lamia, Informatiksicherheitsbeauftragter des Bundes vom Informatikstrategieorgan des Bundes (ISB): «Nach dem Notebook-Diebstahl achteten die Mitarbeiter der Bundesverwaltung plötzlich besonders gut auf ihre Notebooks», ist ihm aufgefallen.

Ihm war aber auch klar: Damit das durch die Katastrophe geweckte Sicherheitsbewusstsein hoch bleibt und weiter steigt, sind

## Hier lesen Sie ...

- wie es um die IT-Security-Awareness der Bundesverwaltung bestellt ist
- wie der Bund den Stand seiner Informationssicherheitskultur gemessen hat
- welche Optimierungsmassnahmen aufgrund der Untersuchung nun ergriffen werden

zusätzliche Aufklärungskampagnen nötig. Doch wo muss man dabei ansetzen? Wie wird die Sicherheit in der Bundesverwaltung wahrgenommen? Kennen die Mitarbeiter die Passwortregeln – und wenden sie diese auch an? Fragen, die sich Lamia zusammen mit Daniel Graf, ebenfalls IT-Sicherheitsbeauftragter des Bundes, schon lange vor dem Notebook-Diebstahl wohl gestellt hatten, auf die sie aber nie ausreichende Antworten erhalten hatten.

Deshalb beschloss das ISB, der Security-Awareness in der Bundesverwaltung mit einer gross angelegten Befragung auf den Grund zu gehen. Diese basierte auf der an der Universität Fribourg entwickelten und vom Spin-off Treesolution optimierten Methode «Twisk» (siehe Kasten).

Per E-Mail erhielten die 30 000 Mitarbeiter der Bundesverwaltung einen Online-Fragekatalog mit 42 Fragen zum Sicherheitsempfinden und -verhalten zugestellt. Rund 2000 beantworteten alle Fragen. Das hört sich nach wenig an. Doch weil sich die Teilnehmer statistisch gleichmässig auf alle Departemente verteilten, seien die Ergebnisse sehr relevant gewesen, interpretiert Lamia den Rücklauf. Zudem könne man aufgrund der wissenschaftlichen Fundiertheit von Twisk annehmen, dass die erhaltenen Daten aussagekräftig seien, pflichtet Graf bei.

## Bauchgefühl bestätigt

Die Ergebnisse der Umfrage haben einerseits das «Bauchgefühl» von Lamia und Graf bestätigt, brachte aber auch überraschende Antworten. So erhielt beispielsweise das Schulungsangebot des ISB schlechte Noten. Die Umfrage-Teilnehmer, das wurde klar, würden durchaus gerne an Kursen teilnehmen, aber nur, wenn diese nicht einen ganzen Tag dauern. Als Sofortmassnahme werden nun auch Halbtageskurse angeboten, ergänzend wird das E-Learning-Angebot überarbeitet und ausgebaut.

Erstaunlich für Lamia und Graf war auch, dass die meisten Befragten bemängeln, es gebe keine eigene Security-Policy. Dabei gibt ebenfalls die Mehrzahl an zu wissen, dass eine «Weisung des Informatikrats Bund über die Informatiksicherheit in der Bundesverwaltung» bestehe. Diese Weisung stellt aber, so Graf, die geforderte Policy dar. Offensichtlich jedoch ist dieses Papier – auch dies ein Ergebnis der Studie – für viele Mitarbeiter zu technisch verfasst und damit nicht verständlich genug.

Als Reaktion plant das ISB nun die Ausarbeitung einer übergeordneten, generellen, nur wenige Seiten umfassenden Policy. «Allerdings muss diese, soll sie ein gewisses Gewicht haben, vom Bundesrat verabschiedet werden», sagt Lamia – und weist damit auf einen Unterschied zwischen der Bundesverwaltung und Wirtschaftsunternehmen hin, in denen solche Dokumente verbindlichen Charakter haben. Lamia hofft, dass bis spätestens Ende 2008 ein entsprechendes Papier vom Bundesrat in Kraft gesetzt wird.

Auch in weiteren Punkten lieferte die Awareness-Umfrage wichtige Antworten. Beispielsweise kennen die Mitarbeiter der Bundesverwaltung zwar die Passwortregeln – halten diese aber in der Praxis nicht immer ein. So kommt es in Einzelfällen vor, dass Passwörter aufgeschrieben und weitergegeben werden. Natürlich geschehen diese Verstösse nicht mutwillig, passierten eher «in der Hitze des Gefechts», erklärt Graf. Beispielsweise dann, wenn ein Mitarbeiter vor seinen Ferien einem Kollegen der Einfachheit halber sein Passwort verrät, anstatt diesem via System ein Stellvertreterpasswort zu geben, um ihm Zugriff auf den eigenen

## «Die Umfrage lieferte uns Erkenntnisse, anhand derer wir künftige Investitionen und Kampagnen besser planen können.»

PC zu verschaffen. Den berühmten, am Monitor klebenden Post-it-Zettel mit dem draufgekritzelten Passwort, gebe es in der Bundesverwaltung aber nicht, so Lamia.

### Unterschiede bei den Departementen

Was es aber gibt, sind klare Unterschiede bei der Sicherheits-Awareness zwischen den Departementen. Lamia und Graf wussten dies zwar – hatten dazu aber keine Zahlen. Nun wissen sie genauer, in welchen Abteilungen es gut und in welchen schlecht aussieht. Wie zu erwarten ist die Awareness in Bereichen, in denen die Leute täglich mit sensiblen Daten umgehen, besser, etwa im Eidgenössischen Departement für Verteidi-

gung, Bevölkerungsschutz und Sport (VBS) und im Eidgenössischen Justiz- und Polizeidepartement (EJPD). Das habe auch damit zu tun, dass die Mitarbeiter hier schon bei der Einstellung eingehend orientiert werden. So muss beim VBS jeder neue Mitarbeiter eine eintägige Informationsveranstaltung besuchen, die auch die IT-Sicherheit thematisiert. Die Studie habe gezeigt, dass diese vorbildliche Praxis auch in anderen Departementen wünschenswert sei.

### «Wir haben etwas in der Hand»

Wichtigstes Ergebnis der Twisk-Untersuchung für Lamia und Graf ist, dass sie nun die Tops und Flops in Sachen IT-Security-Bewusstsein in der Bundesverwaltung konkret benennen und die erzielten Werte mit Benchmarks aus der Industrie vergleichen können.

Auch um Mittel für weitere Massnahmen locker zu machen, sei die Studie, die nur 1.50 Franken pro Mitarbeiter gekostet habe, Gold Wert, wie Lamia betont. «Damit haben wir etwas in der Hand, wenn wir mit Vorschlägen vor den Informatikrat Bund IRB, treten. Und wir können die finanziellen Mittel für Aufklärungskampagnen dort einsetzen, wo sie wirklich die Security-Awareness heben», erklärt er.

Dank der guten Erfahrungen habe man sich vorgenommen, die Twisk-Umfrage in zwei bis drei Jahren zu wiederholen. «Dann können wir überprüfen, was die nun lancierten Massnahmen tatsächlich gebracht haben», freut sich Lamia schon jetzt. ■

### METHODIK UND AUSWERTUNG DER TWISK-UMFRAGE

## So verhilft Twisk zu mehr Awareness in Sachen Informationssicherheit

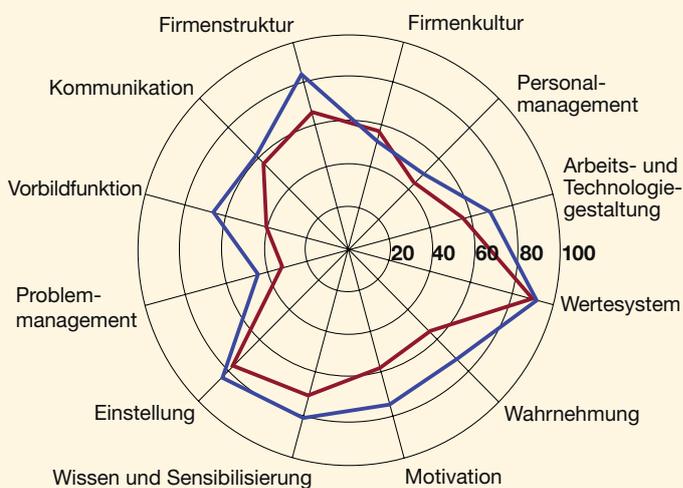
Mit Twisk (Treesolution Werkzeug zum Management der Informationssicherheitskultur) soll die Sicherheitskultur eines Unternehmens in Zahlen gefasst werden. Das Verfahren wurde am International Institute of Management in Technology (IIMT) der Universität Fribourg entwickelt und wird nun vom Spin-off «Treesolution» vermarktet.

Mit Twisk wird zunächst der «Ist-Zustand» der Awareness innerhalb einer Firma eruiert. Zu diesem Zweck wird via Intranet ein Online-Fragebogen mit rund 40 Aussagen zur IT-Sicherheit, zur Firma, den Vorgesetzten und zum eigenen Verhalten zur Verfügung gestellt. Die Mitarbeiter bewerten die Aussagen auf einer fünfstufigen Skala. Zu den abgefragten Aussagen gehören etwa «Neue Mitarbeiter werden über Sicherheitsvor-

schriften informiert», «Mein Vorgesetzter schaut immer und ohne Ausnahme auf konsequente Umsetzung der Sicherheitsrichtlinien» oder «Ich behandle E-Mails von unbekanntem Absendern vorsichtig».

Die aus der Umfrage erhaltenen Werte werden in einem Diagramm dargestellt (Bild rechts), das zeigt, wo Mängel bestehen. Diese lassen sich noch besser visualisieren, wenn man das eigene Diagramm mit dem eines Referenzbetriebs vergleicht. Twisk sollte zudem in gewissen Zeitabständen wiederholt werden. So lässt sich die Effizienz ergriffener Massnahmen zur Steigerung der Security-Awareness überprüfen. Zu den Partnern von Treesolution, die Twisk umsetzen, gehören beispielsweise BW Digi-tronic, Hecom und Ispin.

[www.treesolution.ch](http://www.treesolution.ch)



Das Twisk-Diagramm erlaubt gute Vergleiche, etwa zwischen Bundesverwaltung (rot) und Referenz-Unternehmen aus der Finanzindustrie (blau).