

## Inhalt

- Bericht vom Fachmeeting II/10 vom 9. März 2010 mit Stephan Wehowsky
- Notiz vom 2. Fachmeeting des ASIS Chapters 160 Westschweiz
- Ankündigung des diesjährigen Workshops mit Gloria Reyes
- Ausblick auf die nächsten Fachmeetings
- Termine
- Impressum

## Bericht vom ASIS Fachmeeting am 9. März 2010 mit Stephan Wehowsky

### Open Doors – Warum Sicherheit immer Lücken hat



Immer wieder erlebt man, dass Sicherheitskonzepte lückenhaft sind, Türen also offen stehen. Offene Türen sind wie offene Geheimnisse: Jeder weiss es, aber keiner tut etwas dagegen. Auf diese Weise bekommen Lücken in Sicherheitskonzepten den Charakter der Unvermeidlichkeit.

Welche Türen stehen typischerweise offen? Am häufigsten beklagt wird der Umgang mit Passwörtern. Entweder werden sie so gewählt, dass die kinderleicht zu erraten sind, oder sie werden gleich an den Monitor gepinnt. Oder betriebliche Interna werden bei lautstarken Telefonaten in aller Öffentlichkeit ausposaunt. Zusätzlich gibt es die zahllosen Fälle, in denen bei der Bedienung von Maschinen oder Systemen Sicherheitsvorschriften ignoriert oder umgangen werden.

In solchen Fällen wird schnell von Leichtsinn gesprochen. Dieser Vorwurf ist aber zu oberflächlich. Wenn man genauer hinschaut, erkennt man, dass der Umgang mit Passwörtern nicht rein rational ist. Bei der Wahl der Passwörter spielen Emotionen eine Rolle, und bei dem täglichen Umgang mit ihnen spielen auch die subjektiven Kosten eine Rolle, die die vorschriftsmässige Handhabung verursacht. Und wer in der Öffentlichkeit telefoniert, konzentriert sich auf sein Thema und seinen Gesprächspartner und nicht auf mögliche Zuhörer, die Informationen zweckentfremden könnten. Die Missachtung von Sicherheitsvorschriften wiederum hängt mit dem menschlichen Bestreben zusammen, möglichst effizient Aufgaben zu erledigen und alles, was dabei stört, ausser acht zu lassen.

Offene Türen haben also viele Ursachen, die je für sich genommen durchaus ehrenwert sein können. Mit Vorwürfen und Mahnungen kommt man da nicht weiter. Vielmehr muss man im Einzelfall genau die Motive erfassen, die zu riskantem Verhalten führen. Allerdings gibt es ein grundsätzliches Problem, an dem auch die besten Sicherheitskonzepte scheitern können. Es handelt sich dabei um die Tatsache, dass der Mensch auf der einen Seite nach Sicherheit

strebt, sie auf der anderen Seite aber nicht erträgt. In unserer Gesellschaft erkennen wir dies daran, dass die vergleichsweise hohe Sicherheit in unserem Alltag durch Risikosportarten kompensiert wird. Der Mensch ist ein Risk Seeker. Je sicherer zum Beispiel Autos dank ABS oder ESC werden, desto riskanter wird gefahren.

### **Die Streiche des Denkapparats**

Es ist aber nicht nur die Psychologie des Menschen, die Lücken in Sicherheitskonzepten reiss. Vielmehr spielt uns unser Denkapparat so manchen Streich. Denn er ist nicht immer in der Lage, Risiken objektiv zu bewerten. Manche Risiken bildet er übergross ab, andere ignoriert er. So werden die Gewaltkriminalität oder mögliche Pandemien überschätzt. Risiken dagegen, die im Zusammenhang mit persönlichen Daten entstehen können, werden unterschätzt. Zudem ist unser Denkapparat so konstruiert, dass er das Bekannte auf das Unbekannte und in die Zukunft projiziert. Er tut also, als wäre das, was er kennt, schon die ganze Welt. Daher sind wir auf das Unerwartete grundsätzlich nicht gefasst und sind für „Schwarze Schwäne“, wie Nassim Nicholas Taleb schreibt, nicht gerüstet.

Unserem Denkapparat fällt es auch schwer, eine weitere Ursache für offene Türen angemessen zu analysieren und zu würdigen. Sie besteht in der Tatsache, dass unsere Gesellschaft aus zahllosen Teilsystemen besteht, die alle ihre eigenen Logiken haben. Wenn zum Beispiel in einem Unternehmen eine beeindruckende Zutrittskontrolle installiert ist, im Hof dagegen die Fenster offen stehen, dann liegt das daran, dass dafür jeweils unterschiedliche Entscheidungsträger verantwortlich sind. Ähnliches beobachten wir in den USA: intensive Einreisekontrolle, aber keine Kontrolle der Ausreise. Die Behörden der USA wissen also nicht, wie viele Personen sich nach Ablauf ihrer Aufenthaltsgenehmigung noch im Lande aufhalten. Diejenigen, die über die Budgets entscheiden, setzen also Prioritäten, die mehr mit Abschreckung und Profilierung als mit lückenloser Kontrolle zu tun haben. Darüber klagt wiederum die Polizei. Und an amerikanischen Schulen sind Videoüberwachungsanlagen installiert, ohne dass die Bilder ausgewertet werden. Für den Ankauf sind ganz offensichtlich andere Entscheidungsträger zuständig als für die Organisation des Schulalltags.

### **Offene Gefängnistore**

Die Zersplitterung unserer Gesellschaft in unzählige Teilsysteme ruft die Sehnsucht nach einer vereinheitlichenden Kraft hervor. Es wäre doch schön, wenn alle an einem Strang zögen. Der Garant dafür wird in der Moral gesehen. Deswegen beobachten wir in den vergangenen Jahren speziell in den Medien eine immer stärkere Moralisierung. Probleme der unterschiedlichen Teilsysteme werden auf die einfache Frage nach Gut und Böse reduziert. Das ist in zweifacher Hinsicht risikoreich. Denn die moralisierenden Vereinfachungen blockieren Problemlösungen. Zum anderen wird die Möglichkeit der Gesellschaft, Fehlverhalten zu sanktionieren, überschätzt. In Europa und in den USA sind die Gefängnisse überfüllt und kaum noch finanzierbar. Deswegen werden zum Beispiel in Kalifornien zehntausende von Häftlingen, darunter auch gefährliche Gewalttäter, ohne nähere Prüfung entlassen. Dies geschieht auf Weisung des Obersten Gerichts von Kalifornien, das die Zustände in den Gefängnissen als Verstoss gegen die Menschenwürde erachtet. Der exzessive Gebrauch der Strafen führt also am Ende an den Stellen zu offenen Türen, an denen man sie am wenigsten erwartet und vor allem gewünscht hätte.

Was bedeuten offene Türen für Sicherheitsverantwortliche? Die Ursachen dafür, dass Türen ungewollt offen stehen, lassen sich nicht immer auf den ersten Blick erkennen und mit einfachen Massnahmen oder Weisungen beheben. Darin liegt aber auch eine grosse Chance. Denn die Sicherheitsverantwortlichen bekommen betriebliche Abläufe oder psychologischen Mechanismen der Mitarbeiter besser in den Blick. Dadurch, dass sie mehr Zusammenhänge

erfassen, steigert sich ihr Nutzen für die Unternehmen. Ein gutes Beispiel dafür sind die Logistikketten, die nach dem 11. September lückenlos dokumentiert werden müssen, um den Ansprüchen der Zoll- und Sicherheitsbehörden in den USA und auch in Europa gerecht zu werden. Ursprünglich wurde in den Unternehmen über den zusätzlichen Aufwand und die damit verbundenen Kosten geklagt. Inzwischen aber zeigt sich, dass hierin eine enorme Kompetenzsteigerung liegt. Zum Beispiel erfahren die Unternehmen viel früher von Unregelmässigkeiten. Entsprechend können sie eher darauf reagieren und zum Beispiel Liefer- oder Produktionsausfällen vorbeugen.

So betrachtet sind offene Türen Symptome für Probleme in wirtschaftlichen Unternehmen oder für psychologisch beschreibbare Eigenarten von Menschen, deren näherer Betrachtung sehr aufschlussreich ist und zu Lösungen führt, die insgesamt als Verbesserung wahrgenommen werden.

Stephan Wehowsky

## **Notiz vom 2. Fachmeeting des ASIS Chapters 160 Westschweiz**

### **Guter Start in der Banque Pictet & Cie**



Drew Donovan

Am 4. Mai 2010 fand in der Banque Pictet & Cie das zweite Fachmeeting der Gruppe Westschweiz des ASIS International Chapters 160 Switzerland in Genf statt. Das Treffen wurde von Drew Donovan, Vice Chairman und Facilitator Westschweiz, einberufen und organisiert. Die drei Fachreferate hatten Risk-Management, Travel & Kidnapping Awareness Programs und IT-Physical Security Convergence zum Thema. An dem Fachmeeting nahmen 40 Teilnehmer aus der Westschweiz und René Schwarzenbach, Bernhard Stoll und Stephan Wehowsky aus der Zentralschweiz teil. Das nächste Fachmeeting wird am 5. Oktober 2010 bei Philip Morris in Lausanne stattfinden.

## **Ankündigung des diesjährigen Workshops mit Gloria Reyes**

### **Web 2.0 als Quelle**

Das Internet hat sich zum grössten Datenspeicher der Menschheitsgeschichte entwickelt. Aber der normale Nutzer kratzt nur an der Oberfläche. Wer tiefer in die Geheimnisse eindringen will, benötigt spezielles Wissen. Schon zweimal hat Gloria Reyes Mitgliedern und Freunden des ASIS International Chapters 160 Switzerland vorgeführt, was es heisst, über die richtigen Schlüssel zu verfügen.

Warum das Update? Das Netz entwickelt sich rasend schnell. Entsprechend kommen immer neue Quellen hinzu – und neue Möglichkeiten, diese zu erschliessen.

Das Internet, einst dem passiven Konsum gewidmet, ist nunmehr interaktiv und komplexer geworden. Wie können Ermittler Web 2.0 mit dessen interaktiven Anwendungen einsetzen? Wie recherchiert man im „Hidden Web“? Welche Neuheiten sind für Ermittler relevant? Der Workshop baut auf dem Wissen, das bereits in den zwei vorangehenden Workshops vermittelt wurde. Aber kein Vorwissen ist notwendig, um teilzunehmen.



**Gloria Reyes**, CFE (Certified Fraud Examiner), trainiert investigative Journalisten, Ermittler und Fachpersonal aus dem Bereich Sicherheit und Business Development in der hohen Kunst der Recherche. Ob es darum geht, Ihr Know-How zu schützen, Informationen über den Wettbewerber zu finden, oder Hinweise zu den Aktivitäten von ausländischen Firmen zu suchen, Frau Reyes kennt schnelle, kostengünstige und legale Kniffe, die Sie sofort umsetzen können.

#### **Inhalte:**

- Neue Suchmöglichkeiten bei Google
- Alternativen zu Google
- Deine Freunde sind meine Freunde – Social Networks
- Bookmarks und Wünschlisten
- Ein Bild sagt mehr als 1000 Worte: EXIF und GPS
- Metadaten verstehen
- Mozilla und TOR Privacy – erleichterte Verschlüsselung und Anonymität
- Sicherheitsmaßnahmen: “do not follow“, “do not archive“
- Übung

**Datum:** **Mittwoch, 23. Juni 2010, 13:30 bis 18:00 Uhr**

**Ort:** **H Focus im Lindenpark 16, 6340 Baar**

Das Kompetenzzentrum liegt an der Stadtgrenze Zug/Baar. Die Erreichbarkeit mit den öffentlichen Verkehrsmitteln (Stadtbahnhaltestelle Lindenpark ist direkt vor dem Haus) und mit dem Auto (in 2 min. ab Autobahnanschluss Baar) ist bestens gewährleistet. Bitte nach Möglichkeit mit den öffentlichen Verkehrsmitteln anfahren oder nur mit "Besucher" gekennzeichnete Parkplätze nutzen.

**Ablauf:** 13h30 Workshop Teil I (jeweils 50 min)  
14h30 Workshop Teil II  
15h30 Pause  
16h00 Workshop Teil III  
17h00 Workshop Teil IV  
18h00 Ende

Anschliessend fakultatives Nachtessen in Zug (bitte bei Anmeldung angeben).

**Preis:** (Ganzer Workshop in 4 Teilen)  
CHF 320.-/Person Mitglieder/Gönner Chapter 160  
CHF 390.-/Person Nicht-Mitglieder.

**Anmeldung:**

Vice Chairman: Philip Ryffel, Tel: 043 444 11 44, Fax: 043 444 11 84  
E-Mail: philip.ryffel@bcswitzerland.com

Melden Sie sich baldmöglichst an, die Plätze sind limitiert. Bitte bringen Sie zur Schulung Ihren eigenen W-lan fähigen LapTop mit. Auf Bestellung können Mietgeräte zur Verfügung gestellt werden (Kostenpunkt CHF 30.00) – Bitte bei Anmeldung bekannt geben.

**Ausblick auf die weiteren Fachmeetings 2010**

8. Juni 2010, Nick Mayencourt / Philip Egli, Sicherheitschecks messbar gemacht

7. September 2010, Thomas Dübendorfer, Cybercrime

9. November 2010, Patrik Senn, Krisen und Notfallkommunikation

Die Treffen beginnen jeweils um 16.30 Uhr im Hotel Widder, Zürich, Rennweg 7. Es werden jeweils detaillierte Einladungen versandt.

**Termine**

**Fachmeeting III/2010**

am Dienstag, den 8. Juni 2010,  
von 16.30 bis 18.30 Uhr

**Workshop mit Gloria Reyes**

Das Web als Quelle – Updates  
Mittwoch, 23. Juni 2010, Nachmittag

**Fachmeeting IV/2010**

am Dienstag, den 7. September 2010,  
16.30 bis 18.30 Uhr

**Fachmeeting Westschweiz**

5. Oktober 2010, Lausanne  
Philip Morris International

**Fachmeeting V/2010**

Dienstag, 9. November 2010  
ca. 16.15 bis 18.00

**GV des Chapters 160 Switzerland**

Dienstag, 9. November 2010

**Impressum**

Redaktion: Dr. Stephan Wehowsky, Communication Officer Chapter 160 Switzerland  
[cofficer@asisonline.ch](mailto:cofficer@asisonline.ch)