

## Inhalt

- Bericht vom Fachmeeting I/10 vom 12. Januar 2010 mit Gloria Reyes
- Ausblick auf die weiteren Fachmeetings 2010
- Vorankündigung des diesjährigen Workshops
- Aktivitäten ASIS Westschweiz
- 2010 ASIS International European Volunteer Leadership confirmed
- 9<sup>th</sup> ASIS International European Security Conference
- Termine
- Impressum

## Bericht vom ASIS Fachmeeting am 10. Januar 2010 mit Gloria Reyes

### Know-How-Schutz und Human Intelligence HUMINT



Gloria Reyes ist den Mitgliedern des Schweizer Chapters mit ihren Workshops zur Internetrecherche in bester Erinnerung. Auf dem Fachmeeting drehte Reyes, die Certified Fraud Examiner CFI ist, den Spiess um: Wie können sich Unternehmen am besten vor den Nachforschungen neugieriger Konkurrenten schützen? Eine alte Weisheit besagt, dass der Angriff die beste Verteidigung ist. Entsprechend betonte Gloria Reyes, dass eine genaue Kenntnis der Angriffsmethoden die beste Basis für wirksame Abwehrmassnahmen legt.

Sie bezeichnet das, was es zu schützen gilt, als Know-How – nicht bloss Patente oder geheime Rezepturen, sondern die Betriebsgeheimnisse, die zu einem Wettbewerbsvorteil führen. Das Wissen, über das ein Unternehmen verfügt, ist nicht nur auf elektronischen Datenträgern oder in Aktenordnern gespeichert. Es bestimmt die Verhaltensweisen der Mitarbeiter, es liefert die Themen der firmeninternen Kommunikation und nicht zuletzt spielt es eine grosse Rolle in den Kundenbeziehungen. Den Mitarbeitern oder Kunden ist dabei oftmals gar nicht bewusst, dass sie mit Informationen umgehen, die für Konkurrenten von allergrösstem Nutzen sein können.

Aus der Tatsache, dass das Know-How in die vielfältigen Beziehungen der Mitarbeiter einfließt, ergibt sich ein zentraler Grundsatz für die Abschöpfung: Technische Methoden sind weitaus weniger effizient als Human Skills. In unserer hoch technisierten Welt mutet es im ersten Augenblick paradox an, dass das gute alte Telefon ein wirksameres Instrument sein kann als die ausgefeilten Hackermethoden. Ausgiebig ging Gloria Reyes auf die vielfältigen Möglichkeiten ein, sich menschliche Nachlässigkeit, menschliche Schwächen oder schlicht

Eitelkeit oder Rachsucht zu Nutzen zu machen. Ganz nebenbei geriet dadurch ihr Vortrag zu einem höchst amüsanten Einblick in die Comedie humaine.

80% der Wirtschaftsspionage geht auf das Konto interner Mitarbeiter. Daher ist es immer sinnvoll, sich bei eigenen Nachforschungen dieses Potenzials zu bedienen. Das Problem dabei ist allerdings, dass die Grenzen zwischen legalen und illegalen Methoden der Informationsbeschaffung fließend sind. Ganz sicher ist es nicht verboten, sich die Websites der Mitbewerber anzuschauen. Auch kann ein offiziell angekündigtes Interview die Grenzen der Legalität nicht verletzen. Der graue Bereich beginnt aber schon bei Betriebsbesichtigungen, wenn diese dazu genutzt werden, mehr Informationen abzugreifen, als von den Veranstaltern erwünscht. Die Competitive Intelligence agiert noch im Graubereich, sofern sie sich keiner Methoden wie der Vorspiegelung falscher Identitäten oder anderer Vorwände bedient. Jenseits des Graubereichs ist die Spionage angesiedelt, weil zu ihr zum Beispiel illegale Abhörmethoden oder das widerrechtliche Eindringen in Datennetze gehören.

### **Grauzonen und Überraschungen**

An einem Fall aus dem Jahre 2001 illustrierte Gloria Reyes, wie schwierig es ist, im Einzelfall die Grenzen zwischen legalen und illegalen Nachforschungen einzuhalten. Procter & Gamble hatte damals einem CI-Unternehmen den Auftrag erteilt, Informationen über den Wettbewerber Unilever einzuholen. Es ging um Details zu einem neuen Haarwaschmittel. Dabei durchforstete das Unternehmen Müllcontainer und kontaktierte leitende Mitarbeiter unter dem Vorwand, Marktforschung zu betreiben. In einem aussergerichtlichen Vergleich zahlte Procter & Gamble 10 Millionen USD an Unilever.

Die Lage wird dadurch noch komplizierter, dass einige Länder mit ihren eigenen Geheimdiensten Wirtschaftsspionage betreiben beziehungsweise kommerzielle Dienste damit beauftragen. Zu diesen Ländern gehören die USA, Frankreich, das Vereinigte Königreich, Japan und Russland. In Deutschland und der Schweiz bedienen sich die Regierungen keiner solchen Praktiken.

Es sei unglaublich einfach, an sensible Informationen heranzukommen, resümierte Gloria Reyes ihre eigenen Erfahrungen. Nach dem sie ihre „Hausaufgaben“ gemacht hat – Beschaffung und Auswertung von allgemein zugänglichen Informationen über das jeweilige Unternehmen und die Zielperson – greift sie mit Vorliebe zum Telefon. Dabei wählt sie bewusst Randzeiten, zu denen in der Regel keine Anrufe erwartet werden und zu denen auch keine Sekretärin zwischen ihr und der Ansprechperson sitzt. Das sind die Zeiten wie morgens kurz nach sieben oder am Freitag nach 17:00 Uhr. Eine von mehreren Methoden besteht darin, der Zielperson zu schmeicheln. „Ihr Vortrag, den Sie neulich auf der Marketing Veranstaltung gehalten haben, enthielt vollständig neue Gesichtspunkte und hat mich tief beeindruckt.“ Schon hat man „einen Draht“ und schon ist es möglich, das Gespräch fortzuführen und dabei das eigentliche Thema in Fortführung von Ablenkungsmanövern immer enger zu umkreisen. Gloria Reyes führte zahlreiche Techniken an, unter anderem

- Appell an das Ego der Zielperson
- Ablenken vom Interviewer
- Ableitung des Interesses vom Hauptthema
- Schattenthemen aufbauen und einsetzen

Das funktioniert nicht nur am Telefon. Es lassen sich auch „zufällige“ Treffen in der Lounge eines Flughafens oder auf einer Messe arrangieren. Immer kommt es darauf an, das Ego der

Zielpersonen aufzuwerten. So sollte man den Zielpersonen Gelegenheit geben, ihre Klugheit zu demonstrieren, indem sie zum Beispiel etwas richtig stellen. Oder man bittet sie um einen leicht zu erfüllenden Gefallen. Im Gegensatz dazu lässt sich auch gezielt ein Missbehagen erzeugen, indem man an einer Stelle schweigt. Das Gegenüber möchte diese unbehagliche Situation so rasch wie möglich beenden und ist entsprechend zu weiteren Zugeständnissen bereit. Hinter diesen Techniken stehen nicht nur die Erfahrungen von Gloria Reyes, sondern psychologisch erprobte Verfahren, die in einigen Fachbüchern hervorragend dargelegt worden sind. Am bekanntesten ist die Technik des neurolinguistischen Programmieren NLP, die in einschlägigen Kursen erlernt werden kann und für die es Zertifikate gibt.

Kevin Mitnick, einer der bekanntesten Ex-Hacker in den USA, dem langjährige Gefängnisaufenthalte Zeit und Musse zum Nachdenken beschert haben, hat in seinem Buch „The Art of Deception“ dargelegt, dass 50% aller wichtigen Informationen durch Social Engineering und nicht durch Hacking gewonnen werden. Gloria Reyes fasste einige der Angriffspunkte so zusammen:

Wer kann etwas für sich behalten?  
Wer möchte nicht zeigen, wie klug er ist?  
Wer würde nicht gerne aushelfen?  
Wer stellt nicht sofort etwas richtig?  
Wer kann Schweigen aushalten?

Um diesen Techniken entgegenzuwirken, ist es notwendig, in den Unternehmen alle Ebenen der Mitarbeiterinnen und Mitarbeiter in entsprechende Awareness-Kampagnen einzubeziehen. Unter anderem gehört dazu auch eine Klassifizierung der Informationen bezüglich ihrer Vertraulichkeit. Oftmals ist es Mitarbeitern gar nicht klar, dass sie über Dinge sprechen, die keinesfalls nach aussen dringen dürfen. Klare Strukturen und Bestimmungen für den Umgang mit Informationen und immer wieder erneuerte Trainings zur Abwehr von Social-Engineering-Tricks sind Massnahmen, die heutzutage die IT-Sicherheit und andere Vorkehrungen wie etwa die Zugriffskontrolle ergänzen müssen.

Stephan Wehowsky

### **Ausblick auf die weiteren Fachmeetings 2010**

- 9. März 2010, Stephan Wehowsky, Open Doors – Lücken in Sicherheitskonzepten
- 8. Juni 2010, Nick Mayencourt / Philip Egli, Sicherheitschecks messbar gemacht
- 7. September 2010, Thomas Dübendorfer, Cybercrime
- 9. November 2010, Patrik Senn, Krisen und Notfallkommunikation (angefragt)

Die Treffen beginnen jeweils um 16.30 Uhr. Der Ort wird noch bekannt gegeben. Es erfolgen jeweils detaillierte Einladungen.

## **Vorankündigung des diesjährigen Workshops**

Der nächste Workshop des ASIS Chapters 160 Switzerland wird wieder von Gloria Reyes gestaltet. Sie führt ihr Thema „Das Web als Quelle“ fort und wird die neuesten Entwicklungen der Rechartechniken im Internet praxisnah vermitteln. Die Veranstaltung wird am 23. Juni 2010 nachmittags in Baar stattfinden. Eine Einladung mit Anmeldeformular folgt.

## **Aktivitäten ASIS Westschweiz**

### **Fachmeetings und Networking**

Drew Donovan hat als Vertreter der ASIS-Mitglieder aus der Westschweiz an zwei Vorstandssitzungen des Chapters 160 teilgenommen. Dabei wurden die organisatorischen Details der Zusammenarbeit festgelegt. Drew Donovan fungiert im Vorstand als Facilitator Westschweiz und bekleidet in dieser Eigenschaft neben Philip Ryffel das Amt des Vice-Chairman. Da in der Westschweiz 50 % der ASIS-Mitglieder bereits über die Qualifikation des CPP verfügen, soll der künftige Trainings Officer im Vorstand des Chapters 160 aus diesem Kreis vorgeschlagen werden.

Am 27. Januar 2010 hat es in Genf ein erstes Treffen der ASIS West Working Group gegeben, auf dem Grundzüge der künftigen Entwicklung festgelegt wurden. Man wird sich sehr aktiv um neue Mitglieder bemühen und peilt eine Zahl von 10 an. In diesem Jahr werden zwei Fachmeetings stattfinden. Das erste wird in Genf am 4. oder 5. Mai in der Bank Pictet & CIE in Genf abgehalten, das zweite Fachmeeting wird am 5. Oktober 2010 bei Philip Morris International in Lausanne stattfinden. Im Mai wird es um die Logistik bei der Sicherheitsbetreuung von Führungskräften auf Reisen gehen, im Oktober stehen die ASIS Certification Programme und Trainings auf der Tagesordnung. Details werden im nächsten Newsletter bekannt gegeben.

## **2010 ASIS International European Volunteer Leadership Confirmed**

The President of ASIS International, Joseph R. (*Bob*) Granger, CPP, has appointed the following volunteer leaders to govern ASIS International in Europe:

Godfried Hendriks CPP, Senior Regional Vice President Europe, also 2010 Global Co-Chair Senior Regional Vice Presidents Group

Thomas Vonier, Regional Vice President Region 25 (Netherlands, Belgium, Luxembourg, UK, Ireland, France, Monaco)

Per Lundkvist, CPP, PSP, PCI - Regional Vice President Region 26 (Estonia, Lithuania, Latvia, Denmark, Finland, Iceland, Norway and Sweden)

Roger Warwick, CPP, Regional Vice President Region 27A (Western Balkans, Italy, Spain, Portugal, Malta and Andorra)

Cengiz Gümüştüis, CPP, Regional Vice President Region 27B (Turkey, Greece, Cyprus, Israel, Eastern Balkans, Caucasus)

Dr. Christoph Rojahn, Regional Vice President Region 28 (Austria, Switzerland, Germany, Russia, Hungary and Liechtenstein)

Dr. Ivan Moroz, Regional Vice President Region 29 (Czech Republic, Slovakia, Poland, Ukraine, Belarus)

The role of an ASIS Regional Vice President (RVP) is –among others - to provide assistance, guidance, and advice to all chapters within his or her region, promote the organisation of new chapters in the region and to promote the welfare, growth, professional prestige, influence, and professional educational development of ASIS within the region.

## **9th ASIS International European Security Conference**



Detaillierte Informationen erhalten Sie unter

<http://www.asisonline.org/education/programs/lisbon/default.htm>

## **Termine**

### **Fachmeeting II/2010**

am Dienstag, den 9. März 2010  
von 16.30 bis 18.30 Uhr

### **Fachmeeting III/2010**

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

### **Fachmeeting IV/2010**

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

### **Fachmeeting V/2010**

Dienstag, 9. November 2010  
ca. 16.15 bis 18.00

### **Fachmeeting Westschweiz**

4. oder 5. Mai 2010, Genf  
Bank Pictet & CIE

### **Workshop mit Gloria Reyes**

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

### **Fachmeeting Westschweiz**

5. Oktober 2010, Lausanne  
Philip Morris International

### **GV des Chapters 160 Switzerland**

Dienstag, 9. November 2010

Die Veranstaltungsorte werden mit den Einladungen bekannt gegeben.

## **Impressum**

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