ISACA®
Trust in, and value from, information systems
Switzerland Chapter
Nr. 02 | Juni 2012 | www.isaca.ch
NEWSLETTER

**Cyberangriffe**
Die Melde- und Analysestelle Informationssicherung befasst sich mit Gefahren im Internet **Seite 73**

**Risikomanagement**
Die CRISC-Zertifikat zeigt die wachsende Bedeutung des Risikomanagements.
**Seite 75**

**ISACA-Training**
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 77**

# Bekämpfung von Cyberangriffen

Die Melde- und Analysestelle Informationssicherung MELANI ist vom Bundesrat mit dem Schutz Kritischer Infrastrukturen in der Schweiz beauftragt und befasst sich täglich mit den Gefahren, die im Internet lauern.

Von Pascal Lamia

Täglich werden private Internetnutzer, aber vor allem auch grosse, mittlere und kleine Unternehmen Opfer von Cyberangriffen. Meist bleiben diese Angriffe über längere Zeit unerkannt, weshalb der durch die Angreifer verursachte ideelle, materielle und finanzielle Schaden ins Unermessliche steigen kann. In Einzelfällen mussten zuvor durchaus erfolgreiche und renommierte Unternehmen Konkurs anmelden, nachdem sie Opfer von Cyberangriffen wurden.

Was aber bezwecken die Angreifer? Grundsätzlich ist immer davon auszugehen, dass jemand, der etwas Verbotenes im Internet tut, damit Geld verdienen will. Dies geschieht oft auf direktem Weg, beispielsweise durch so genannte «Man-in-the-Middle»-Angriffe im E-Banking: Den Angreifern gelingt es mithilfe eines zuvor auf dem PC des Opfers installierten Schadprogramms parallel zur E-Banking-Sitzung des Opfers eine zweite Sitzung aufzubauen und so – vorläufig unbemerkt – illegal Geld auf ausländische Konten zu transferieren. Geld lässt sich aber auch verdienen, indem beispielsweise Betriebsgeheimnisse, Baupläne für ein neues Produkt, chemische Zusammensetzungen für neue Medikamente usw. entwendet werden. Diese Informationen lassen sich im Untergrundmarkt problemlos zu Geld machen.

Wer denkt, dass er oder sie als private/r Internetnutzer/in für Angreifer nicht interessant ist, liegt falsch: Immer häufiger wird z.B. der Missbrauch von Kreditkartendaten oder der so genannte Identitätsdiebstahl: Eine Person gibt sich für illegale Zwecke als eine andere, real existierende Person aus. Dies ist beispielsweise eine der Motivationen, die hinter den allseits bekannten Lotto-Mails stehen: Diese Mails stellen Ihnen oft einen Gewinn in Millionenhöhe in Aussicht, jedoch müssen Sie als «Bestätigung» eine Kopie Ihres Passes einscannen und per Mail zurückschicken. Die so übermittelten Personalien dienen den Betrügern, um sich für illegale Machenschaften als eine andere, real existierende Person auszugeben.

Sehr beliebt sind momentan Mails, die ein Betrüger im Namen einer anderen Person abschickt: Der Betrüger hat zuerst das E-Mail-Konto eines unbeschadeten

Bürgers – nennen wir ihn Karl Mustermann – gehackt und sich so Zugang zu den im E-Mail-Konto gespeicherten Kontakten verschafft. Der Betrüger verschickt im Namen von Karl Mustermann Mails, in denen er seine Bekannten, Freunde und Geschäftspartner um Hilfe bittet: Er sei im Ausland ausgeraubt worden und benötige dringend Geld für die Bezahlung der Hotelrechnung und für den Kauf eines Tickets in die Heimat. Man solle das Geld bitte via Western Union an ihn überweisen.

Andere Betrüger greifen zu weitaus dreisteren Mitteln: So machte beispielsweise vor einigen Monaten eine E-Mail im Namen einer real existierenden Anwaltskanzlei in Deutschland die Runde: Den Empfängern wurde mitgeteilt, sie hätten illegal MP3-Songs vom Internet heruntergeladen und auch Songs ins Internet hochgeladen. Eigentlich – so die «Anwaltskanzlei» müsse man Anzeige wegen Verstosses gegen das Urheberrechtsgesetz erstatten, würde aber bei der Bezahlung eines kleineren dreistelligen Betrages absehen. Viele Personen, die dieses Mail erhalten haben, haben auch tatsächlich bezahlt, weil sie sich vor einer Anklage fürchteten.

**Im Vergleich zu den folgenden Beispielen mögen die oben erwähnten Vorfälle richtig harmlos klingen:**
Vor rund zwei Jahren sorgte der Computerwurm «Stuxnet» für weltweites Aufsehen: In einem iranischen Urananreicherungswerk wurde dieser Computerwurm entdeckt. Er war so raffiniert programmiert, dass er nur ganz bestimmte Systeme eines einzigen Herstellers befiel. In der Folge manipulierte er die Drehzahl der für die Urananreicherung notwendigen Turbinen. Diese Turbinen müssen in einem sehr konstanten Drehzahlbereich arbeiten. Stuxnet reduzierte und erhöhte die Drehzahl der Turbinen mehr oder weniger beliebig, während er den Ingenieuren im Kontrollraum gleichzeitig vorgaukelte, die Drehzahl sei sehr konstant. Im Extremfall hätten die Turbinen erheblichen Schaden nehmen und unter Anderem sogar Uran freigesetzt werden können. Analysen des Computerwurms haben ergeben, dass eine einzige Person für die Programmierung rund 10 Jahre hätte aufwenden müssen. Diese und weitere Erkenntnisse lassen vermuten, dass ein oder mehrere ausländische Staaten in diesen Angriff involviert waren oder ihn sogar selber durchgeführt haben.

Selbstverständlich ist auch die Bundesverwaltung nicht vor Angriffen gefeit: So gelang es Angreifern im 2009 in das Netzwerk der Bundesverwaltung einzudringen. Auch in diesem Fall waren die Vorbereitungsarbeiten für die Angreifer sehr hoch und die programmierte Malware wurde explizit für diesen Zweck gebaut. Daher steht auch hier die Vermutung im Raum, dass einer oder mehrere ausländische Staaten an diesem Angriff beteiligt waren.

Die Frage steht natürlich im Raum, ob und wie man sich gegen solche Vorfälle effizient schützen kann. In erster Linie sollten alle Personen das Internet mit der gebotenen Vorsicht verwenden und sich bewusst sein, dass jedes Unternehmen und jede Privatperson für Angreifer interessant ist. Daneben müssen selbstverständlich die gängigen Sicherheitsmassnahmen umgesetzt werden: Aktueller Virenschutz, regelmässige Updates von Betriebssystem und Anwendungen, im Unternehmensbereich ebenfalls klar definierte Firewall-Policies, deren Umsetzung regelmässig überprüft wird.

Damit jedoch nicht genug: Die Erfahrung zeigt, dass technische Massnahmen allein nicht genügen, um sich insbesondere vor Informationsdiebstahl zu schützen: Es reicht nicht aus, beispielswiese das Anschliessen von externen Datenträgern wie z.B. USB-Sticks zu verbieten und die USB-Ports zu deaktivieren. Heute verfügt fast ausnahmslos jedes Handy über eine Sprachaufzeichnungsmöglichkeit, über eine Foto- und Filmkamera. In besonders sensiblen Bereichen sollte daher auch die Frage geklärt werden, ob, von wem und unter welchen Voraussetzungen Handys in diese Unternehmensbereiche mitgebracht werden dürfen.

Die Problematik der mobilen Geräte, egal ob Handy oder Tablet, werden uns in Zukunft noch vermehrt beschäftigen. Einen wirklich adäquaten Schutz gibt es nämlich nicht und die neuen Generationen solcher Geräte werden immer schneller und verfügen über eine grosse Speicherkapazität. Das heisst, es werden in Zukunft immer mehr geschäftliche Informationen auf diesen Geräten bearbeitet; ein Unterschied, ob vertraulich oder nicht wird oftmals nicht gemacht, Hauptsache man kann flexibel arbeiten. Die Sicht einer integralen Informationssicherheit wird zur grossen Herausforderung und braucht pragmatische, aber sichere Lösungen.

Pascal Lamia, Leiter MELANI

## DER AUTOR

**Pascal Lamia** ist Leiter der Melde- und Analysestelle Informationssicherung MELANI sowie Informatiksicherheitsbeauftragter des Bundes. Er ist 44 Jahre alt und arbeitet seit Jahren im Informatikbereich.

Information des Verbandes

# Risikomanagement

Eine seriöse Aus- und Weiterbildung wie CRISC ist dringend nötig

Der separate Beitrag von Pascal Lamia, Leiter MELANI, zeigt auf, dass wir gerade im Internet zahlreichen Risiken ausgesetzt sind. Dies gilt nicht nur für Privatpersonen sondern in vermehrtem Masse auch für Unternehmungen. Diese sollten sich daher im Rahmen eines systematischen Risikomanagements umfassend mit der Identifikation, Bewertung und Bewältigung der verschiedenen Risiken beschäftigen.

Eine nicht-repräsentative Stichprobe in verschiedenen kleineren und grösseren Unternehmungen hat aufgezeigt, dass zwar viele ein sogenanntes Enterprise Risk Management (ERM) haben, dieses aber nur sehr rudimentär implementiert ist. Das heisst z.B., dass einerseits die im ERM geführten Risiko-Szenarien eher oberflächlich bestimmt und bewertet wurden. Anderseits sind die Beschreibungen dieser Szenarien dermassen knapp, dass man sich darunter bei jeder der periodischen Neubewertungen immer wieder etwas komplett Anderes vorstellen kann, wodurch eine konsistente Bewertung und Planung risikomindernder Massnahmen faktisch unmöglich ist.

Im Informatik-Umfeld ist das nicht zwangsläufig anders: Auch hier werden die Risikoregister sehr oberflächlich geführt und die notwendigen Verbesserungsmassnahmen rein situativ und keineswegs systematisch ermittelt. Oft werden auch Restrisiken ohne formale Genehmigung akzeptiert, welche eigentlich jenseits des (definierten) Risikoappetits liegen.

Ein Hoffnungsschimmer ist jedoch am Horizont erkennbar. In nicht einmal zwei Jahren haben weltweit fast 18,000 Personen das neue ISACA-Zertifikat im Bereich Risikomanagement und IKS im IT-Umfeld CRISC (Certified in Risk Management and Information Systems Control) erworben – ein geradezu sensationelles Ergebnis. Ganz offensichtlich ist das Interesse am CRISC-Zertifikat riesig, welches die insgesamt 39 verschiedenen Aufgaben eines Risikomanagers in den fünf übergeordneten Themenbereichen abdeckt: Ein Schwerpunkt des Berufsbilds bilden die Identifikation, Einschätzung und Bewertung von Risiken sowie deren Management und Überwachung. Der zweite Schwerpunkt bilden Design und Implementation von IT-Kontrollen sowie deren Überwachung und Unterhalt. In dieser Kombination deckt das neue CRISC-Berufsbild und die entsprechende Zertifizierung ein offensichtliches Markt-Bedürfnis ab. Gerade diese neue Gattung von Risiko- und Kontrollspezialisten CRISC könnte in Zukunft dafür sorgen, dass solche wie in der Einleitung erwähnten Mängel deutlich seltener werden.

Nicht nur das neue CRISC-Zertifikat zeigt die wachsende Bedeutung des Risikomanagements. So wurde zum Beispiel im neuen «Business Framework for the Governance and Management of Enterprise IT» COBIT 5 das Risikomanagement deutlich höher gewichtet und ein komplett neuer Governance-Prozess «EDM03 Ensure Risk Optimisation» eingeführt. Das neue Standardwerk kann übrigens von www.isaca.org gratis heruntergeladen werden.

Das ISACA Switzerland Chapter führt ab Juli 2012 bereits zum vierten Mal einen CRISC-Kurs durch (13 Kurstage verteilt über 4–5 Monate). Der berufsbegleitende Kurs richtet sich an alle Personen, die sich mit unterschiedlichsten Risikomanagementfragen und Frameworks oder mit dem Design, der Implementation, der Überwachung und Wartung von Sicherheitsmassnahmen und anderen Kontrollen beschäftigen – also Risikomanager und Sicherheitsbeauftragte innerhalb und ausserhalb der IT, Compliance-Officer, IKS-Verantwortliche, erfahrene Informatikrevisoren, IT-Anwendungsentwickler oder Projektcontroller.

Der Kurs vermittelt und vertieft theoretisches wie praktisches Fachwissen im breiten Feld von Risikomanagement und internen Kontrollen, bereitet aber auch intensiv auf die von ISACA organisierte CRISC-Prüfung vor.

## WEITERE INFORMATIONEN

Weitere Details zum CRISC-Zertifikat und zur entsprechenden Ausbildung finden Sie auf www.isaca.ch


## IMPRESSUM ISACA NEWS

| | |
|---|---|
| **Herausgeber, Redaktion:** | ISACA Switzerland Chapter |
| **Adresse:** | Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich |
| **Erscheinungsweise:** | 4x jährlich in Swiss IT Magazine |
| **Mitgliedschaft:** | Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch |
| **Copyright:** | © Switzerland Chapter der ISACA |

# Preisgekröntes ISACA Switzerland Chapter

Das ISACA Switzerland Chapter wurde bereits mehrfach ausgezeichnet. Die neu gestaltete Webseite wurde nun mit einer Gold-Medaille prämiert.

Von Peter Bitterli

Das ISACA Switzerland Chapter gehört mit den unterdessen 1,250 Mitgliedern zu den sehr grossen «Töchtern» des internationalen Fachverbandes ISACA, der insgesamt weit über 100,000 Mitglieder aufweist. Das ISACA Switzerland Chapter wurde 1988 als Verein gegründet und richtet sich an Personen aus verschiedensten Bereichen der Informationstechnologie (IT), welche sich mit Sicherheit, Risikomanagement, Governance oder Assurance beschäftigen. In den letzten Jahren haben wir zunehmend Mitglieder in Führungsfunktionen dazugewonnen, welche für Governance-Aspekte verantwortlich sind.

Das ISACA Switzerland Chapter wurde für seine Leistungen gegenüber den Mitgliedern bereits mehrfach ausgezeichnet – z.B. für das letzte Vereinsjahr als «bestes sehr grosse Chapter von Europa & Afrika». Auch die komplett neu gestaltete Webseite wurde mit einer Gold-Medaille ausgezeichnet. Weltweit einzigartig sind auch die 13- bis 15-tägigen, berufsbegleitenden Ausbildungen sowie die grosse Zahl an professionellen Kursen.

Heute ist die ISACA zusammen mit dem IT Governance Institute der Knowledge-Provider für IT Governance, IT Risk Management, IT Assurance und IT Security. Die ISACA setzt sich in professioneller Art mit allen Entwicklungen in diesen Themenbereichen auseinander und macht ihre diesbezüglichen Erkenntnisse interessierten Kreisen weltweit zugänglich. Zu den bekanntesten Produkten gehören die international anerkannten Standards COBIT 5®, Val IT™ und Risk IT.

Wer noch nicht die Gelegenheit hatte, das neue Governance-Framework COBIT 5 anzuschauen: Laden Sie sich von www.isaca.org Ihre persönliche Kopie herunter – es lohnt sich! Die neueste COBIT-Version wurde noch deutlicher auf die Steuerung der IT aus Unternehmenssicht ausgerichtet: von der Geschäftsleitung (über die Balanced Score Card) bis hinunter in die verschiedenen Tätigkeiten innerhalb der Informatik und über das neue, auf ISO 15504 basierende, Process Assurance Modell PAM zur Messung der Prozessleistung wieder zurück in die Teppichetage. Dabei wurden andere zentrale Frameworks wie ITIL (Service Management), TOGAF (Architektur) oder ISO27000 (Informationssicherheit) in der COBIT-Version 5 wesentlich besser integriert resp. berücksichtigt.

Schauen Sie einmal bei uns vorbei – auf unserer Webseite **www.isaca.ch** oder auch einmal bei einer unserer zahlreichen Veranstaltungen.

## ALS ISACA-MITGLIED KÖNNEN SIE VON FOLGENDEN VORTEILEN PROFITIEREN

- Zugriff auf ISACA's internationale Standards, Frameworks, Guidances, Practices, Benchmarks und Tools, sowie auf das IT Professional Networking and Knowledge Center, dem Treffpunkt für IT-Fachleute mit diversen Informationsaustausch- und Kollaborationsmöglichkeiten.
- Möglichkeit zur Teilnahme an gratis-online-Kursen zu Themen im Bereich IT Governance, Control, Security, Risk, Audit
- Rabatte bei sämtlichen nationalen und internationalen ISACA-Konferenzen
- Rabatte bei den Zertifikatsprüfungen CISA, CISM, CGEIT und CRISC
- Rabatte auf dem Sortiment des ISACA Bookstore
- Periodische Informationen via E-Mail und der Zeitschrift «ISACA Journal»
- Rabatte auf sämtlichen Kursen der ITACS Training AG
- Ausgezeichnete Vorbereitungsunterlagen und Kurse mit international anerkanntem Zertifikat für CISA, CISM, CGEIT und CRISC (Ausbildung sowie Prüfungsvorbereitung)
- After Hours-Seminare zu aktuellen Themen: monatlich in Zürich und 3–4 Mal pro Jahr in Genf oder Lausanne; für Mitglieder jeweils gratis
- Möglichkeit zur Mitarbeit in verschiedenen Interessengruppen, welche spezifische Themen behandeln und Hilfsmittel (z.B. Prüfprogramme, Checklisten) erarbeiten
- Für deutschsprachige Mitglieder gratis die Fachzeitschrift «Swiss IT Magazin» mit der Möglichkeit, selber darin Artikel zu platzieren
- Durch das Switzerland Chapter herausgegebene eNews (10 mal pro Jahr)
- Enge Zusammenarbeit mit den grossen Revisionsgesellschaften, der Schweizerischen Treuhand-Kammer, Educaris (der Akademie der Treuhand-Kammer), dem Schweizerischen Verband für interne Revision (SVIR) sowie mit anderen Schweizer IT Security-Organisationen (siehe www.swisssecurity.org).Damit verbunden sind hauptsächlich ein gegenseitiger Informationsaustausch und teilweise gemeinsame Veranstaltungen (mit entsprechenden Vergünstigungen).

# Interessengruppen – Aktive Teilnahme möglich!

Das ISACA Switzerland Chapter bietet die Möglichkeit, bestimmte Themen zusammen mit Experten aus verschiedenen Bereichen vertieft zu bearbeiten und zu erforschen. Dies geschieht via sogenannter Interessengruppen (IG). Die jeweilige IG setzt sich ihre Ziele selber. Diese sollen jedoch im Zusammenhang mit Themen aus dem ISACA-Umfeld sein. Wichtig ist zu wissen, dass die - von den ISACA-IGs erarbeiteten Ergebnisse nach ihrer Fertigstellung in Form einer «Zusammenfassung» den ISACA-Mitgliedern und im Idealfall der Öffentlichkeit - uneingeschränkt zur Verfügung stehen. Es wird dadurch Mehrwert für alle Members generiert und dafür wird die IG von ISACA unterstützt, vor allem bezüglich Administration, Organisation und Räumlichkeiten.

Auf Wunsch werden die Beteiligten im Ergebnisdokument namentlich erwähnt. Eine Veröffentlichung in den eNews oder den ISACA-Seiten des Swiss IT Magazins, im Rahmen - eines ISACA After Hours-Seminares oder einer anderen Veranstaltung wird durch das ISACA-Vereinssekretariat sowie den Vorstand fachlich und organisatorisch unterstützt.

**Das ISACA Switzerland Chapter verfolgt folgende Ziele mit IGs:**

- Attraktive IGs zu aktuellen Themen für ihre Mitglieder, um auf dem neusten Stand zu sein
- Aktuelle Information der ISACA-Mitglieder über die von den IGs aktuell bearbeiteten Themenbereichen
- Wecken des Interessens der Mitglieder aufgrund interessanter Themen, sich ebenfalls an einer der IGs zu beteiligen
- Einbringen von neuen und interessanten Themenvorschlägen durch die ISACA-Mitglieder
- Wahrnehmung von ISACA in all ihren Bereichen und nicht nur im IT-Audit-Umfeld
- Bessere Nutzung des Know-hows der ISACA-Mitglieder

Haben Sie ein brennendes Thema? Sind Sie interessiert, es vertieft zu bearbeiten und zudem mit Erfahrungen aus der Praxis anzureichern?

## WEITERE INFORMATIONEN

Ich hoffe, ich habe Ihr Interesse geweckt. Besuchen Sie doch die ISACA-Webseite **www.isaca.ch**, um sich einen Überblick über die aktuellen IGs zu verschaffen. Hier finden Sie ebenfalls die neuen Regeln.

Haben Sie einen Themenvorschlag für eine IG oder möchten Sie uns Feedback geben, dann senden Sie uns eine Mail an: **interestgroups@isaca.ch**

Das ISACA Switzerland Chapter freut sich auf Ihre Unterstützung bei einer der existierenden IGs und ist offen für neue und interessante Themenvorschläge.

## ISACA-TRAINING

| Datum | Code | Hauptthema – Kurstitel |
|---|---|---|
| 4.6.2012 | GL-SAP | **Grundlagen zur Prüfung von SAP-Systemlandschaften** |
| 5.-6.6.12 | BK-SAP | **Prüfung des Berechtigungskonzeptes von SAP-Systemen** |
| 7.-8.6.12 | SP-SAP | **Systemprüfung von SAP-Systemen** |
| 11.6.12 | OUT-KK | **Risiken, Überwachung und Prüfung von Outsourcing-Providern** Bekommen Sie Ihr Outsourcing in den Griff - speziell auch für KMUs |
| 13.6.12 | SM-EY | **Social Media effizient prüfen und in den Griff bekommen** Nutzen und Risiken erkennen und wirksame Management-Prozesse einführen |
| 28.-29.6.12 | MT-BL | **IT Governance for Mobile Technology (English)** |
| 2.7.12 | SN-BL | **Social Networks in the Business World - Risk or Reward? (English)** |
| 3.7.12 | CC-BL | **Introduction to Cloud Computing (English)** |
| 4.7.12 | CO-BL | **Introduction to COBIT 5 (English)** |
| 5.7.12 | PAM-BL | **COBIT Process Assessment Model PAM (English)** |
| 11.-13.7.12 | PM-BJ | **Projektmanagement-Knowhow für Nicht-Projektleiter** Softwareentwicklungsprojekte optimal begleiten und prüfen |
| 6.7.-13.11.12 | CISA-VK | **CISA-Zertifikatskurs 2012\|2** Vertiefungskurs IT-Revision, IT-Kontrolle, IT-Sicherheit, IT-Governance und CISA-Prüfungsvorbereitungskurs. Offizieller CISA-Kurs des ISACA Switzerland Chapter |
| 6.7.-14.11.12 | CISM-VK | **CISM-Zertifikatskurs 2012\|2** Vertiefungskurs Konzeption, Governance und Management der Informationssicherheit, Risiko-Management, Reaktionsmanagement und CISM-Prüfungsvorbereitungskurs. Offizieller CISM-Kurs des ISACA Switzerland Chapter |
| 6.7.-15.11.12 | CGEIT-VK | **CGEIT-Zertifikatskurs 2012\|2** Vertiefungskurs IT-Governance: strategische Ausrichtung, Wertschöpfung, Risikomanagement, Ressourcen-Management und Leistungsmessung und CGEIT-Prüfungsvorbereitungskurs Offizieller CGEIT-Kurs des ISACA Switzerland Chapter |
| **www.glenfis.ch** | | |
| 11.-12.6.12 | COB-IG | **ISACA Implementing Governance of Enterprise using COBIT (Deutsch)** |
| 18.-20.6.12 | COB-FB | **ISACA COBIT 4.1 Foundation Zertifikat** |

**Das gesamte Trainingsangebot mit näheren Informationen finden Sie online unter www.isaca.ch**