

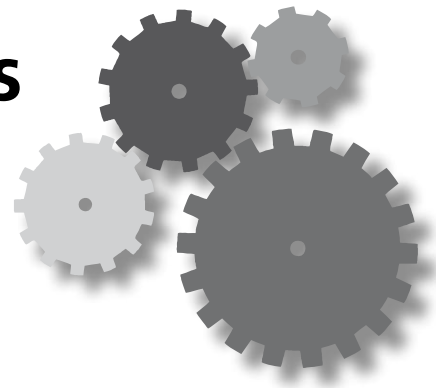
Mit Grundschutz bestens vorbereitet

Interview mit Isabel Münch, Referatsleiterin für Systemsicherheit und IT-Grundschutz, BSI

Elmar Török, bits+bites

Dipl.-Math. Isabel Münch ist seit 1994 beim Bundesamt für Sicherheit in der Informationstechnik (BSI), zurzeit als Referatsleiterin für Systemsicherheit und IT-Grundschutz.

Ihre Arbeitsschwerpunkte sind die Weiterentwicklung der IT-Grundschutzkataloge, außerdem vertritt sie das BSI in verschiedenen nationalen und internationalen Gremien mit dem Schwerpunkt IT-Sicherheitsmanagement.



Isabel Münch, Referatsleiterin für Systemsicherheit und IT-Grundschutz, BSI

IT-Grundschutz: Frau Münch, die Bedrohungen in der IT entwickeln sich ständig weiter, wie passen Sie die Kenntnisse der ISO 27001-Auditoren für Audits auf der Basis von IT-Grundschutz daran an?

Münch: Die Kenntnisse der Auditoren müssen sich an den Grundlagenwerken, also den ISO-Normen und dem IT-Grundschutz orientieren, das ist das oberste Gebot. Natürlich passen wir die Ausbildung kontinuierlich an, eben weil neben den ISO-Normen auch IT-Grundschutz und BSI-Standards geändert oder erweitert werden. Wir sind dabei durchaus flexibel. Wenn sich über die zwei planmäßigen Schulungstermine im Jahr hinaus Bedarf ergibt, dann setzen wir weitere Termine an.

IT-Grundschutz: Woher kommen die größten Veränderungen? Tragen Firmen auch mit Vorschlägen dazu bei?

Münch: Von der Industrie bekommen wir zwar häufig Anmerkungen zu den IT-Grundschutzkatalogen und den Standards, aber kaum direkten Input zum Ausbildungsinhalt, das ist schade. Wenn sich da konkrete Anfragen ergeben würden, diskutieren wir die selbstverständlich. In der Regel sind natürlich Änderungen an den Standards die Auslöser für eine Veränderung der Ausbildungsinhalte. Es gibt drei große Faktoren, einmal die ISO 2700x Reihe, die ständig überarbeitet wird. Dann gibt es die Änderungen an den IT-Grundschutz-Standards, so stehen bald wieder Neuigkeiten beim BSI-Standard 100-2 an. Und zu guter Letzt müssen wir Anpassungen bei den Zertifizierungs- und Auditierungsschemata beachten.

IT-Grundschutz: Soll das Konzept so bleiben oder planen Sie für die Zukunft Änderungen an der Vorgehensweise?

Münch: Generell ist das eine Praxis, die sich sehr bewährt hat. Es gibt daher wenig Anreiz, grundlegend zu reformieren. Außerdem können wir einiges an der Ausbildung gar nicht antasten, es sind ja auch Vor-

gaben durch die ISO-Normen, auf die wir keinen Einfluss haben. Diskutiert wird aber beispielsweise die organisatorische Abwicklung. Die Schulungen sind auf eine Woche mit 40 Stunden ausgelegt. Dafür ist der Themenkanon schon sehr ehrgeizig, unsere Teilnehmer sprechen gern von einer Powerschulung. Es gibt einfach viel Stoff, der vermittelt werden muss. Da kommt immer mal wieder die Frage, ob wir nicht auf sieben Tage verlängern sollen, aber dann ist eben eine zweite Woche notwendig und das ist für viele Teilnehmer schwer mit den Anforderungen des Arbeitgebers vereinbar.

IT-Grundschutz: Reicht denn die Menge der am Markt verfügbaren Auditoren aus? Oder sind eher zu viele Personen zertifiziert?

Münch: Die Erfahrung mit den Institutionen zeigt, dass es zur Zeit ausreichend Auditoren gibt, um die Nachfrage nach IT-Grundschutz-Zertifizierungen oder Beratungen zu decken. Aber wir wollen die Anzahl der Auditoren in keiner Weise regeln oder in den Markt eingreifen. Es darf auch nicht vergessen werden, dass bei Weitem nicht alle der zertifizierten Auditoren für Institutionen zur Verfügung stehen. Viele der Absolventen durchlaufen die Ausbildung, weil sie in ihrer

eigenen Institution IT-Grundschutz implementieren und betreuen wollen. Solche Auditoren sind zunächst nicht für andere Firmen oder Behörden greifbar.

IT-Grundschutz: Das Ausbildungskonzept erfordert Praxiserfahrung im Vorfeld. Ist das für die Teilnehmer machbar? Neben dem normalen Job und dessen Anforderungen?

Münch: Die zukünftigen Auditoren müssen nicht ausschließlich Zertifizierungen absolviert haben, aber generell ist die Praxiserfahrung Teil der ISO-Anforderungen. Sie kann auch durch vorbereitende Audits oder Audits aus anderen Bereichen erlangt werden. Wichtig ist, dass die Teilnehmer generell Erfahrungen im Umgang mit Zertifizierungen gesammelt haben, auch wenn vielleicht keine komplette Zertifizierung begleitet worden ist.

IT-Grundschutz: Das BSI stellt hohe Anforderungen an die zukünftigen Auditoren. Lohnt sich das für die Absolventen persönlich?

Münch: Ja, absolut. Ganz abgesehen davon, dass fachlich viel Wissen vermittelt und aufgenommen wird, hat das Auditoren-Zertifikat einen hohen Stellenwert bei den Institutionen. Die Absolventen können damit regelrecht Werbung machen und profitieren ganz klar davon. Es ist eben auch bekannt, dass dieses Zertifikat mit viel Aufwand verbunden ist und nicht inflationär verteilt wird.

IT-Grundschutz: Und das wird auch in der Industrie mit steigender Nachfrage quittiert?

Münch: Das ist in der Tat so. Wir verzeichnen eine zunehmende Menge an Nachfragen von Institutionen nach Auditoren und ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz. Das hat natürlich mehrere Gründe. Bestimmt spielt die Sicherheitsla-

ge eine Rolle, die durch zahlreiche öffentlichkeitswirksame Attacken sensibler gesehen wird. Aber ein Zertifikat ist nun mal auch ein sehr einfacher und schneller Nachweis über die Erfüllung von bestimmten Anforderungen. Bei vielen Firmen, aber auch Behörden, gibt es Kunden, Partner und auch Aufsichtsstellen, die als Erstes die notwendigen Zertifikate abfragen. Früher hatte man sich gegenseitig versichert, dass man die richtigen Dinge tut, heute muss man – aus Gründen der Compliance – auch nachweisen, das dem wirklich so ist. Ein Zertifikat ist dabei der einfachste und schnellste Weg.

IT-Grundschutz: Das klingt ein bisschen, als ob man Verantwortung abwälzen möchte.

Münch: Nein, beim Wunsch nach Zertifizierung spielt eine wesentliche Rolle, nachvollziehbare und transparente Bewertungen von Experten als Basis für eigene Entscheidungen einzuholen. Gut kann man das im Moment beim Thema Cloud-Computing sehen, wo wir uns vor Anfragen nach Zertifizierungsmöglichkeiten kaum retten können. Das Konzept ist für viele interessant, aber man will die Sicherheit am besten durch ein Zertifikat bestätigt wissen.

IT-Grundschutz: Wie sieht es mit anderen Zertifizierungen aus?

Münch: Auch für die anderen Zertifizierungen, die wir anbieten, steigt die Nachfrage konstant an. Im letzten Jahr ergab die vom Infodienst IT-Grundschutz durchgeführte Studie, dass Interesse an einer Personenzertifizierung für IT-Grundschutz-Experten besteht und wir diskutieren das seitdem intern sehr intensiv. Auch für den BSI-Standard 100-4 gibt es sehr häufig Anfragen, die sich eine Zertifizierung des Notfallmanagements von Institutionen wünschen. Wir stehen dem absolut positiv gegenüber. Wenn der Markt so etwas verlangt, dann

sehen wir unsere Aufgabe darin, die Industrie zu unterstützen. Das sind schließlich auch Wettbewerbsvorteile im Vergleich mit anderen Ländern.

IT-Grundschutz: Frau Münch, IT-Grundschutz gibt es seit mehr als 15 Jahren, trotzdem ist nur ein Bruchteil der Unternehmen zertifiziert. Muss der Gesetzgeber mehr Druck auf die Firmen ausüben?

Münch: Wir sehen keine Notwendigkeit für Gesetze. Es gibt wirklich ausreichend gute Gründe, um IT-Grundschutz umzusetzen und ohnehin bereits viele Gesetze, die Unternehmen verpflichten, ein angemessenes Sicherheitsmanagement umzusetzen, wie KonTraG oder Basel II bzw. III. Dadurch ist der legislative Druck völlig ausreichend, um im Management die Bereitschaft für die Umsetzung von Sicherheitsmaßnahmen zu wecken. Generell glaube ich auch nicht, dass es ein grundsätzliches Problem mit der Umsetzungsbereitschaft des IT-Grundschutz gibt. Viele sind aktiv und agieren bereits in der richtigen Richtung, andere haben noch Nachholbedarf.

IT-Grundschutz: Was ist Ihrer Erfahrung nach die größte Umsetzungshürde bei der Durchführung einer ISO 27001-Zertifizierung?

Münch: Selten ist es die technische Seite, da sind die meisten bereits gut aufgestellt, Defizite lassen sich schnell beheben. Es ist eher die Etablierung des IT-Sicherheitsmanagements als solches. Es gibt häufig noch keine schlüssige und funktionierende Integration der IT-Sicherheit in die Geschäftsprozesse. Manchmal hat sich auch die Funktion des IT-Sicherheitsbeauftragten noch nicht richtig etabliert. Und die Unterstützung der Leitungsebene ist nicht überall ausreichend.

IT-Grundschutz: Nimmt das Management die Risiken nicht wahr?

Cyber Security 2011

Schutz kritischer Informationen

30. Mai – 01. Juni 2011 | Pullman Berlin Schweizerhof

Risiken – Prävention – Technologien – Strategien

Besuchen Sie unser Download Center für kostenfreie Whitepaper, Artikel und vieles mehr!
www.cyber-security-konferenz.de/MP

Themenschwerpunkte:

- aktuelle Risiken der Wirtschaftsspionage und mögliche Präventionsmaßnahmen
- Bedrohungsanalyse als Bestandteil der Risikoanalyse
- Schutzkonzepte kritischer Infrastrukturen
- Identitiy Management und Authentifizierungsmöglichkeiten

Hören Sie Praxisberichte zu Szenarien und Schutzkonzepten für Mobile Security und Cloud Computing, um Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

Informieren Sie sich auf unserer Webseite auch über unsere sicherheitstrategischen Workshops

www.cyber-security-konferenz.de/MP

Jetzt in NRW

public IT

Fachmesse für kommunale IT-Lösungen und Dienstleistungen

12.-13. April 2011
Messe Düsseldorf

ONLINE REGISTRIEREN LOHNT SICH
www.public-it-messe.de/registrierung

HIGHLIGHTS DER MESSE:

- ▶ Hochkarätige Vorträge in Zusammenarbeit mit renommierten deutschen Universitäten und Hochschulen
- ▶ PPP-Konferenz des Finanzministeriums NRW moderiert von Prof. Dr. H. W. Alfen, Bauhaus-Universität Weimar (im Eintrittspreis integriert, separate Anmeldung erforderlich)

50%
DES PREISES
SPAREN

Das Programm finden Sie ab Februar unter
www.public-it-messe.com

Zeitgleich mit

public 11

3. internationale Fachmesse für Stadtplanung und öffentliche Raumgestaltung

Partner

Finanzministerium
des Landes Nordrhein-Westfalen



Fraunhofer
FOKUS

4th Pan-European Conference

IT Compliance 2011

Frameworks, Policies and Procedures. Audits. Effectiveness. Metrics. Information security.

Berlin, Germany, 29th & 30th June 2011

Selected Speakers:

Antonio Lombroso
Internal Control, Head ICT
Audit Service
Banca MPS S.p.A., Italy

Mikael May Yde
Head of Department IT
Compliance, Corporate IT
Lundbeck, Denmark

Tim Plona
Corporate Information Security Officer /
ICT Compliance Officer CIST
Océ-Technologies, Netherlands

Per Silberg Hansen
Chief Information
Security Officer
ECCO Sko, Denmark

Mit freundlicher Unterstützung von: Media Partner:

betasystems



For more information please contact: **Izzet Maral**
E-Mail: Izzet.Maral@marcusevansde.com Tel: +49 (0)30 890 61 240
Fax: +49 (0)30 890 61 434 www.marcusevansde.com

marcusevans conferences



Open Source mobilisiert.

13. Mai: Security Day
by Astaro mit großem HackingContest!

RedHat, Gartner und Google sagen:
Die Zukunft ist offen.

Der LinuxTag stellt es unter Beweis.

Open Source ist Geschäftsmodell,
ist Arbeitgeber & Trendsetter.
Zahlreiche Unternehmen & Projekte
sowie namhafte Speaker der Branche
sind sich einig.

**LINUX
TAG**

11.-14. Mai 2011 in Berlin
**EUROPE'S LEADING
OPEN SOURCE EVENT**
CONFERENCE | EXHIBITION | PROFESSIONAL DEVELOPMENT

www.linuxtag.org



Messe Berlin

Münch: Oft ist einfach nicht klar, was so eine Zertifizierung an Anforderungen und Nachweisen erfordert. Daraus können sich dann Widerstände ergeben, weil der entstehende Aufwand höher ist als erwartet. Häufig wünscht das Management sogar selbst eine Zertifizierung, senkt dann aber den Daumen, wenn der IT-Sicherheitsbeauftragte mitteilt, welcher Aufwand dahinter steckt.

IT-Grundschutz: Also ist der Zeitaufwand zu hoch?

Münch: Das kann man so nicht sagen. Im Prinzip ist eine ISO 27001-Zertifizierung in sechs Wochen machbar, das hängt aber wesentlich von der geleisteten Vorarbeit ab. Eine gut vorbereitete Institution, die interne Experten ausreichend ausgebildet hat oder einen qualifizierten Berater hinzugezogen hat und bei der auch schon im Vorfeld ein schlüssiges IT-Sicherheitsmanagement herrschte, kann das eigentliche Audit sehr schnell abschließen. Aber natürlich kann es auch länger dauern, je nachdem, was vorher noch in die richtigen Bahnen gelenkt werden muss.

IT-Grundschutz: Reicht der Bekanntheitsgrad des IT-Grundschutz aus? Vor allem kleine und sehr kleine Unternehmen haben noch nie von den IT-Grundschutzkatalogen gehört.

Münch: Meiner Ansicht nach ist das Thema im Großen und Ganzen in der Industrie angekommen, Nachholbedarf gibt es vielleicht noch bei den Mittelständlern. Aber es gab und gibt viele Kampagnen der Bundesregierung, mit denen genau diese Zielgruppe erreicht werden soll. Das Thema Verbreitung wird von uns nicht vernachlässigt, es gibt nur eine riesige Menge von Firmen, gerade im Mittelstand. Hier wird es immer wieder Unternehmen geben, die wir erst noch erreichen müssen.

IT-Grundschutz: Gibt es genug Anbieter von Schulungen zum Thema IT-Grundschutz?

Münch: Ja, aus unserer Sicht sind ausreichend Anbieter von IT-Grundschutz-Schulungen am Markt vertreten. Wir sehen das auch an der abnehmenden Zahl von Nachfragen nach Schulungen durch das BSI. Die Liste der Schulungsanbieter für IT-Grundschutz auf unserer Webseite wächst. Und auch die Qualität scheint gut zu sein. Zudem hat das BSI begonnen Web-Kurse zu bestimmten Themen anzubieten, zum Beispiel zur IT-Grundschutz-Vorgehensweise, zum GSTOOL und zum Notfallmanagement nach BSI-Standard 100-4. Auch hier ist die Nachfrage enorm, das zeigt uns, dass es ein akzeptiertes Medium für die Informationsvermittlung ist.

IT-Grundschutz: Das BSI bietet neben der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz auch weitere Zertifizierungen an, beispielsweise für IT-Sicherheits-

dienstleister, die Penetration-Testing anbieten. Wird das vom Markt angenommen?

Münch: Generell ist die Antwort „Ja“. Wir haben beispielsweise mittlerweile um die 250 Audit-Teamleiter für ISO 27001, über 100 IT-Revisoren und die ersten acht De-Mail Auditoren sind ebenfalls schon geprüft worden. Im Bereich Penetrationstests laufen die Zulassungsverfahren gerade, hier sind auf unserer Seite noch ein paar Schritte zu leisten. Aber besonders für die Penetrationstester ist die Nachfrage vonseiten der Kunden riesig. Bei einem so stark auf Vertrauen basierenden Service ist es absolut essentiell, dass die beteiligten Personen so viele Referenzen mitbringen wie irgend möglich. Und eine Zertifizierung durch das BSI gilt als besonders wichtig.

IT-Grundschutz: Frau Münch, wie sehen Sie die weitere Entwicklung des Bereichs Auditoren-Ausbildung und Zertifizierung beim BSI?

Münch: Die Zertifizierung ist einer der Grundpfeiler des BSI, nur durch Zertifikate können Nachhaltigkeit, Nachvollziehbarkeit und Vertrauenswürdigkeit in die IT-Sicherheit nachgewiesen werden. Daran wird sich auch in Zukunft nichts ändern.

IT-Grundschutz: Frau Münch, wir danken Ihnen für dieses Gespräch. ■

Die kompletten Ergebnisse

Studie IT-Sicherheitsstandards und IT-Compliance

Die kompletten Ergebnisse jetzt bestellen:

80 Seiten,
A4 gebunden,
zahlreiche Grafiken
und Tabellen,
295,00 €
zzgl. Versandkosten

www.grundschutz.info/studie

oder per Tel. +49 6725 9304-0



Gratisabruf Video-Slideflow:
www.grundschutz.info/webcast



IT-Grundschutz



Bundesamt
für Sicherheit in der
Informationstechnik



research
an der Universität
Regensburg GmbH

Die Umfrage entstand in Zusammenarbeit der Zeitschrift „Informationsdienst IT-Grundschutz“ mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und ibi research.