

Summary SecurityRadar 2011



Editorial



„Sie erhalten mit dem SecurityRadar ein Instrument an die Hand, das Ihnen erlaubt, Ihre eigene Arbeit in einen Benchmark zu setzen und zu wissen, wie und wo Ihr Unternehmen im Schweizer Umfeld einzuordnen ist.“

Marco Marchesi

Liebe Leserinnen und Leser des SecurityRadar 2011,

Sie halten nun die Summary unserer 2. schweizweiten Befragung zu IT- und Informationssicherheit in Ihren Händen. Es geht uns darum, Ihnen ein objektives Bild zu IT- und Informationssicherheit, Risikomanagement, Datenschutz und verwandten Gebieten aufzuzeigen. Ergänzend dazu ziehen wir die Ergebnisse ausgewählter internationaler Sicherheitsstudien zu einer vergleichenden Betrachtung heran.

Die Zusammenstellung interessanter und wertvoller Erkenntnisse ist uns in diesem Jahr erneut gelungen. Wir legen besonderen Wert auf Objektivität und Realitätsbezug. Wie ein Radar werden wir Ihnen Orientierung und Übersichtlichkeit in einem komplexen Themengebiet bieten. Sie erhalten mit dem SecurityRadar ein Instrument an die Hand, das Ihnen erlaubt, Ihre eigene Arbeit in einen Benchmark zu setzen und zu wissen, wie und wo Ihr Unternehmen im Schweizer Umfeld einzuordnen ist. Jedes Jahr wählen wir Schwerpunktthemen. So standen 2010 die Themen Datenschutz und Information Security Management sowie SIEM im Fokus. Dieses Jahr haben wir dem Umgang und Risiko sozialer Netzwerke und Business Continuity Management (BCM) mehr Raum gegeben.

Im gesamten Studienband erhalten sie alle detailliert und präzise ausgewerteten Ergebnisse – kommentiert von Experten aus der Branche. So bekommen Sie einen umfassenden Überblick über die Sicherheitslandschaft in Schweizer Unternehmen und alle relevanten Fakten zum Thema Informationssicherheit.

Ich wünsche Ihnen nun viel Freude und eine Menge neuer hilfreicher Erkenntnisse beim Lesen der Summary. ■

Herzliche Grüsse
Ihr Marco Marchesi,
CEO der ISPIN AG ZURICH

Highlights und Auszüge aus den Ergebnissen des SecurityRadar 2011

Mitarbeitende werden immer noch als **ein hohes Sicherheitsrisiko** gesehen – allerdings nicht mehr mit gleicher Relevanz wie im Jahr 2010.

Bewusstseinsbildung für Mitarbeitende wird stark gefordert. Bei 20% der Befragten stehen **Awareness-massnahmen** immer noch nicht auf der Roadmap.

Professionalisierte Angriffe auf die firmeneigenen Netzwerke, aber auch die anarchistische Vorgehensweise einzelner „**Hacktivisten**“ bereiten Schweizer Sicherheitsverantwortlichen deutlich grössere „**Bauchschmerzen**“ und werden als sehr viel höher und risikoreicher eingeschätzt als noch 2010.

Die **wichtigsten Themen** in Schweizer Informationssicherheitsabteilungen: Einhaltung rechtlicher Vorgaben, der Schutz von Unternehmens- und Markenreputation sowie die Sicherstellung des Datenschutzes bzw. des Schutzes von Personendaten.

Top-Risikothemen im Unternehmen: Datenverlust, nicht autorisierte Zugriffe auf die eigenen Systeme und Verfügbarkeitskrisiken. Die Informationssicherheit hat in vielen Unternehmen noch „**Überwachungsfunktion**“, weniger ist sie Treiber für Anforderungen aus dem Business.

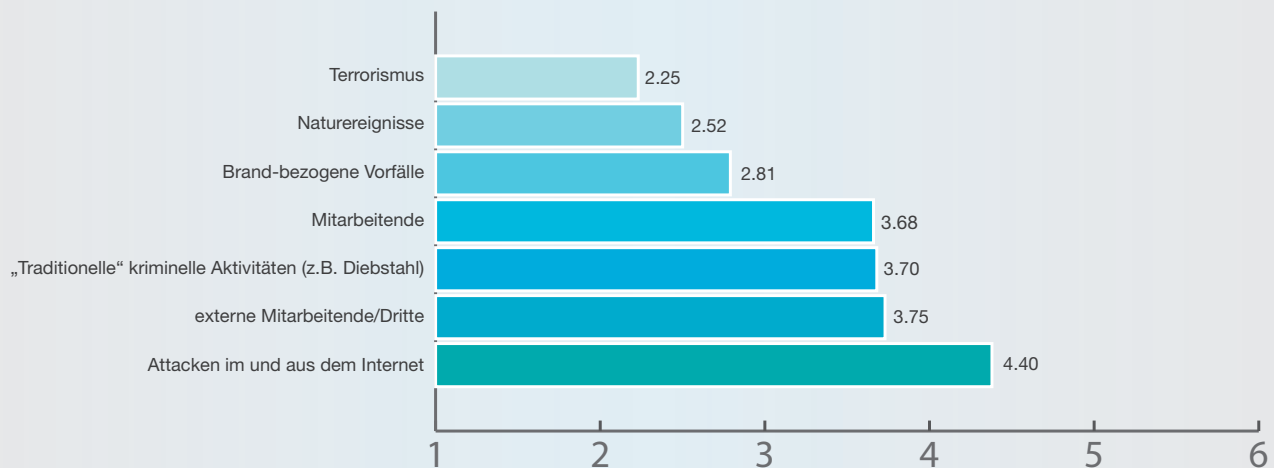
Eine gewisse Hilflosigkeit ist deutlich ausmachen. Gegenüber der Professionalisierung von Angriffen von Ausen, sehen sich viele Sicherheitsverantwortliche **eher schutzlos ausgeliefert**.

Wieviel Kontrollverlust muss man als einkalkulierbares Risiko auf sich nehmen? Der Verlegung von Unternehmensdaten und Anwendungen in die „**Cloud**“ stehen viele Befragte sehr kritisch gegenüber.



Ranking "Risiken für Unternehmen"

(1 = tiefes Risiko, 6 = hohes Risiko)



© 2011 ISPIN AG ZÜRICH

Die steigende Komplexität der IT-Infrastrukturen in Schweizer Unternehmen treibt den Sicherheitsbeauftragten immer stärker den Schweiß auf die Stirn.

Reputationsrisiken sind genau so wichtig gewertet wie andere Risikoarten. Fast die Hälfte aller befragten Unternehmen hat bereits das Thema Reputationsrisiko in die unternehmenseigene **Risikomanagement-Strategie** integriert oder befindet sich hier im Umsetzungsprozess.

Mehr als die Hälfte aller Unternehmen haben bereits Social Media Richtlinien etabliert. Ein aktives **Monitoring**, um sich einen Überblick über die Aktivitäten in sozialen Netzwerken zu verschaffen, betreiben nur die Wenigsten.

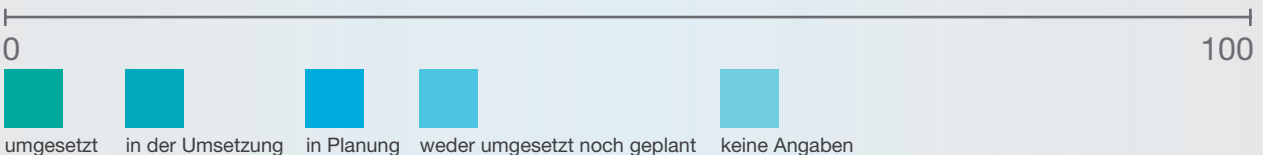
Business Continuity Management (BCM) ist in vielen Unternehmen ein Thema – allerdings ohne die notwendige hohe Priorisierung. In BCM-Projekten fehlt es oft an **bewusstseinsbildenden Massnahmen** bei den Mitarbeitenden und dem **Testen der Pläne** – wenn sie dann vollständig sind – bzw. Übungen mit dem **Krisenstab** oder dem Krisenmanagementteam.

Nur knapp 40% der Befragten schätzen ihre unternehmensinternen Notfallpläne auch als effektiv ein.

Sicherheitsabteilungen spüren immer stärker den Kostendruck und die Sparsbremse. Als Herausforderung bei der Umsetzung von ausgewählten Security Initiativen, rangiert **angemessenes Budget** an zweiter Stelle gleich hinter der **Verfügbarkeit von qualifizierten Mitarbeitenden** und noch vor der **Schaffung eines Bewusstseins für Informationssicherheit** im gesamten Unternehmen. ■

Themen umgesetzt, in Umsetzung, in Planung, weder noch:

Unified Computing System	5,63	9,86	18,31	38,03	28,17		
Cloud Security	8,11	14,86	6,76	52,70	17,57		
Outsourcing interner Securitydienste	20,55	5,48	5,48	56,16	12,33		
Privileged User Monitoring	9,59	23,29	17,81	36,99	12,33		
Database Encryption	17,57	14,86	13,51	41,89	12,16		
Unified Communication	20,83	15,28	18,06	26,39	19,44		
Managed Security Services	22,22	15,28	6,94	44,44	11,11		
File/Folder Encryption	21,62	16,22	16,22	35,14	10,81		
Data Loss Prevention / Data Leakage Prevention	24,66	23,29	17,81	27,40	6,85		
Secure Data Exchange/Collaboration	34,25	16,44	12,33	27,40	9,59		
Network Encryption	35,14	17,57	9,46	31,08	6,76		
Network Access Control	32,43	21,62	17,57	21,62	6,76		
Strategic Security Planning	38,89	12,50	18,06	23,61	6,94		
Single Sign ON	38,67	16,00	16,00	26,67			
Pentesting	46,67	10,67	12,00	21,33	9,33		2,67
Social Media Policies	37,84	18,92	21,62	18,92			2,70
Business Impact Analyse	42,11	22,37	13,16	11,84	10,53		
Logging, Monitoring, Alerting, Reporting (SIEM)	40,79	18,42	19,74	17,11	3,95		
End Point Security	47,95	12,33	12,33	21,92	5,48		
Security Awareness	41,33	25,33	16,00	14,67			2,67
Web Entry Security	57,53	10,96	12,33	10,96	8,22		
Identity & Access Management	43,42	30,26	15,79	6,58	3,95		
Information Risk & Security Management	47,95	28,77	12,33	5,48	5,48		
Risiko Assessment	57,33	16,00	18,67	4,00	4,00		
IT-Governance, Compliance, IKS	56,76	24,32	6,76	8,11	4,05		
Vulnerability- & Patch-Management Service	56,94	25,00	6,94	8,33			2,78
Business & IT Service Continuity	53,33	29,33	10,67	2,67	4,00		
Virtualisierung	76,71	9,59	6,85	2,74	4,11		
Datenschutz	71,62	21,62	1,35	2,70			2,67
Netz- & Security Infrastrukturen	74,67	16,00	4,00				2,67



Themenübersicht des SecurityRadar 2011

– das erwartet Sie im Studienband

- ⊞ Informationssicherheit in Schweizer Unternehmen (allgemein)
- ⊞ Risiken erkennen und managen (inkl. Schwerpunktthema I: Social Media)
- ⊞ Der Faktor Mensch und (Security) Awareness
- ⊞ Compliance, Governance & Datenschutz
- ⊞ Schwerpunktthema II: Business Continuity Management & Notfallvorsorge
- ⊞ Normen & ISMS
- ⊞ Security-Projekte: Planung, ToDo und Umsetzungsstrategien
- ⊞ Ressourcen & Budgets
- ⊞ Studiengrundlage / Demografische Daten



NETBREEZE

Qualitativ erweitert wird der SecurityRadar in diesem Jahr mit einer Online-Trendanalyse „Sicherheit“, welche wir mit unserem Online-Monitoringpartner NETBREEZE AG erstellen. Rapportiert wird über Sicherheitsthemen und Dienstleister aus diesem Bereich. Somit bekommen Sie eine Gesamtschau darüber, welche Sicherheitsthemen in der Fachwelt via Online-Newsportalen, Twitter, Facebook oder Foren gerade im letzten Jahr aktiv diskutiert wurden. Der hier eingesetzte ComMonitor der NETBREEZE AG unterstützt uns auch in der Realisierung unseres Reputation Management Service. Wenn Sie hierzu Fragen haben, setzen Sie sich einfach direkt mit uns in Verbindung.

ISPIN AG ZURICH
swiss made security.®

www.ispin.ch

Kontakt und Anfragen zum SecurityRadar 2011

Marcus Beyer und Katja Dörlemann

Studienteam des SecurityRadar 2011

mail: securityradar@ispin.ch

ISPIN AG ZURICH

Grindelstrasse 15

CH-8303 Bassersdorf

Tel.: +41 44 838 31 11