

SecurityRadar 2011

Leseprobe BCM

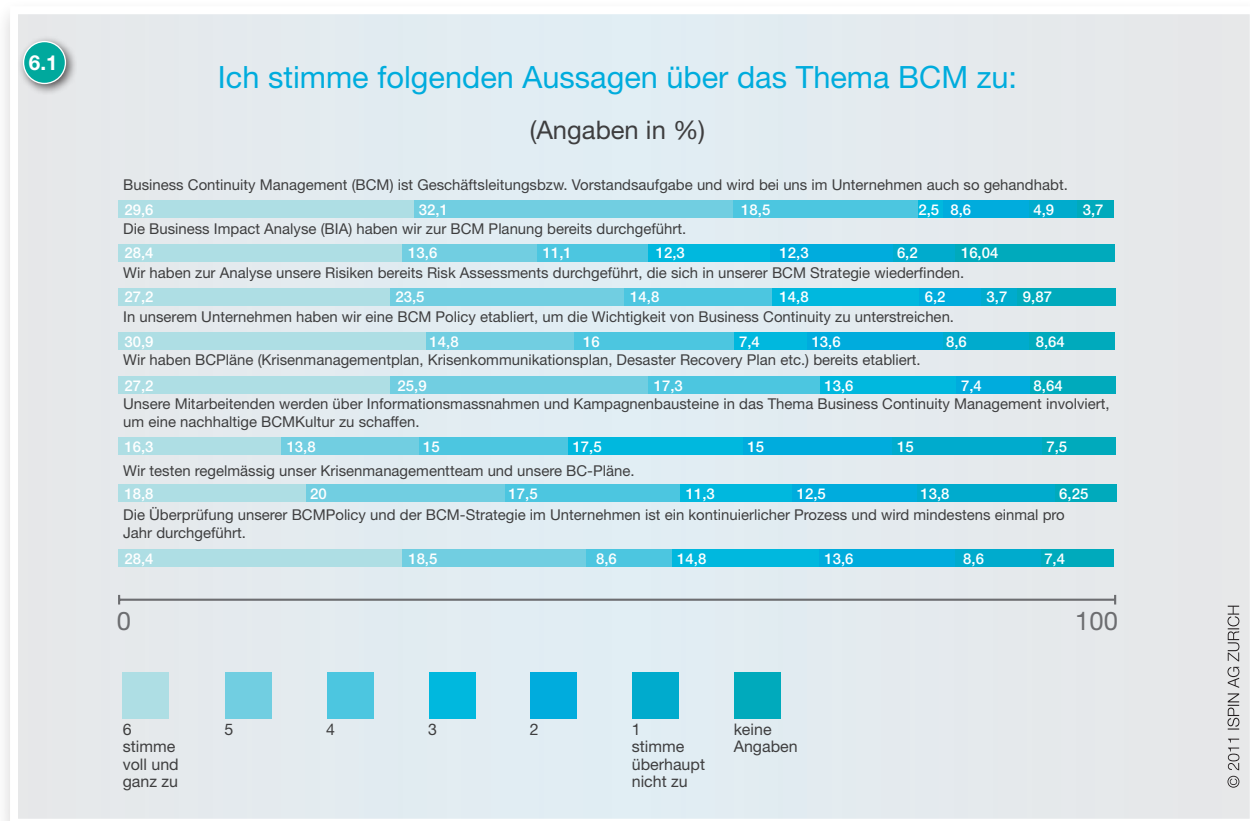


Kapitel VI – Business Continuity Management und Notfallvorsorge

„Es stellt sich immer wieder die Frage, wo sich „Informationssicherheit“ abgrenzt und führt auch zu entsprechenden Diskussionen, wenn es um die Verantwortlichkeiten und Kompetenzen geht bei diesem Thema.“

Business Continuity Management (BCM) sei durchaus Thema in den Unternehmen – allerdings oftmals noch ohne die notwendige Priorisierung, die das Thema aus den Erfahrungen der letzten Monate geniessen müsste, so Marcus Beyer, Senior Architect Security Awareness bei der ISPIN AG ZURICH. Fukushima ist bereits aus dem Blickfeld verschwunden.

Bei rund 80% der befragten Unternehmen ist das Business Continuity Management Geschäftsleitungs- bzw. Vorstandsaufgabe und wird auch so praktiziert. In den meisten Fällen wird BCM also top down realisiert, wodurch die Durchsetzungskraft dieses Themas vergrössert wird. Problematisch ist hier, die einzelnen wichtigen Bereiche für ein funktionierendes BCM auch angemessen zu berücksichtigen und keinen zu vernachlässigen (→Abb. 6.1).



Es ist eindeutig zu erkennen, dass die Grundlagen für ein funktionierendes BCM in den meisten Unternehmen vorhanden sind. Knapp über die Hälfte der Befragten (53.1%) gibt an, dass ihr Unternehmen bereits eine Business Impact Analyse (BIA) zur BCM-Planung durchgeführt hat. 56,3% testen regelmässig ihr Krisenmanagementteam und ihre BC-Pläne und bei 55.5% ist die Überprüfung ihrer BCM-Policy und BCM-Strategie ein kontinuierlicher Prozess, der mindestens einmal pro Jahr vorgenommen wird. „Diese Ergebnisse widersprechen meinen Erfahrungen in der täglichen Arbeit bei Kundenunternehmen“, wundert sich allerdings Ivan Allemann, Head Business Security und Compliance bei der ISPIN AG ZURICH, „Audits und Überprüfungen werden in der Praxis nämlich nur sehr selten durchgeführt.“ Im hiesigen Rahmen berücksichtigt werden muss, dass die Befragten aus dem IT-Umfeld heraus antworten. Trotzdem sei, so Ivan Allemann, Testing, das über eine probenhafte Evakuierung des Gebäudes hinaus geht, also ein Testing, das an die tatsächlichen Businessprozesse heranreicht, leider noch sehr unüblich. Schon 65,5% der hier repräsentierten Unternehmen haben sich internen Risk Assessments unterzogen, die dann in die BCM-Strategie integriert wurden. Eine BCM-Policy haben mit 61,7% ebenfalls über die Hälfte der Unternehmen etabliert, um damit die Wichtigkeit des Themas zu unterstreichen. Ebenso existieren bei den meisten hier befragten Unternehmen BC-Pläne (Krisenmanagementplan, Krisenkommunikationsplan, Disaster Recovery Plan etc.). Im Annual Security Report 2010 betont Cisco die immense Bedeutung eines Incident Response Plans. Demnach muss ein Unternehmen wissen, was im Ernstfall zu tun ist. Ein effektiver Incident Response Plan hilft, die Auswirkungen eines Vorfalles einzudämmen, sichert die korrekte Handhabung und lässt zusätzlich ein Lernen aus Fehlern zu. Dazu muss er aber eben effektiv und anwendbar sein.

Das Involvement der Mitarbeitenden über Informationsmassnahmen und Kampagnenbausteine ist bei den meisten Firmen leider nicht üblich. Damit verpassen sie allerdings die Chance, auf allen Ebenen des Unternehmens eine nachhaltige BCM-Kultur zu schaffen. Awareness sollte eben nicht Anfang und Ende im Themenbereich IT-Security finden. Die Unterstützung eines wissenden Mitarbeitenden ist für alle Bereiche des Unternehmens nützlich und erstrebenswert. „BCM-Awareness darf nicht auf die leichte Schulter genommen werden“, rät Marcus Beyer, Senior Architect Security Awareness bei der ISPIN AG ZURICH, „im Krisenfall, in dem schnelles und korrektes Verhalten gefordert ist, wissen die Leute sonst nicht, was zu tun ist.“ Wie im Bereich Security-Awareness ist auch hier die Kommunikationsproblematik präsent. Es ist unklar wem, wann, was und wie kommuniziert werden soll.

Nur 32% der Befragten geben an, dass die Notfallpläne ihres Unternehmens effektiv sind. Der meist genannte Grund für die nicht genügende Effizienz bestehender Notfallpläne in Unternehmen ist die Unvollständigkeit des Planes (26%). Auch die verzögerte Umsetzung (16%) oder die fehlende Unterstützung des Managements (13%) werden häufig als Grund für eine eingeschränkte Funktion der Notfallpläne genannt (→ Abb. 6.2).

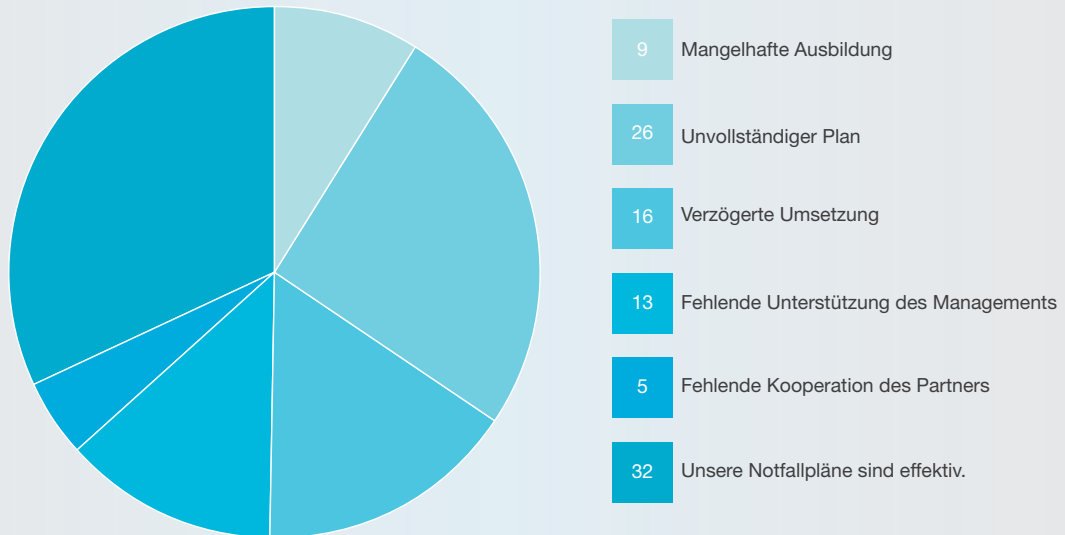
In den Ergebnissen zum Punkt ‚Mangelhafte Ausbildung‘ (‚Lack of training‘) gehen die sonst sehr wohl vergleichbaren Befunde der weltweiten PwC-Studie und der hier vorliegenden auseinander. Seltener hingegen ist für Schweizer Unternehmen eine unzureichende Kompetenz der Mitarbeitenden als Grund für die Ineffektivität der Notfallpläne – die weltweit befragten Unternehmen geben dies aber am häufigsten an!

Ebenfalls in der Befragung sichtbar ist, dass das tatsächliche Testen der Notfall- und Krisenstabspläne immer noch stiefmütterlich behandelt wird. „Sie werden eben nicht auf ihre Handhabbarkeit im ganzen Unternehmen hin überprüft“, weiss Marcus Beyer zu berichten. Tritt ein Notfall oder eine Krise ein, können nur 32% der Unternehmen handeln, 62% liefern auf ein Disaster zu. „Hier besteht absoluter Handlungsbedarf“, legt er mit Nachdruck nahe.

Ganze 83% geben an, Business & IT Service Continuity entweder umgesetzt oder in der Umsetzung zu haben (→ Abb. 8.1). Wir stossen wieder auf das gleiche Problem: Abteilungsübergreifende Prozesse sind mühsam. „Sobald es um interdisziplinäre Zusammenhänge geht, sind viele verloren“, resümiert Marcus Beyer. Auch hier gilt, die Umsetzung eines erfolgreichen BCMs Schritt für Schritt zu forcieren. Oft bleibt ein mit viel Aufwand erstelltes Konzept nur auf dem Papier, weil die praktische Umsetzung zu teuer, zu zeitaufwendig, zu komplex ist. „Wie bei dem Thema Datenschutz muss hier stufenweise vorgegangen werden“, rät Ivan Allemann, Head Business Security und Compliance bei der ISPIN AG ZURICH, „besonders in Unternehmen, die die Massnahmen personell und finanziell nur schwer stemmen können.“ ■

Die Notfallpläne unseres Unternehmens waren aus folgenden Gründen nicht genügend effektiv:

(Angaben in %)



Bestellung

Der ausführliche Studienband enthält alle Fragen sowie die kommentierten Ergebnisse des ISPIN Security Radar 2011 und ist für CHF 470,00 über securityreport@ispin.ch bestellbar.

Alternativ können Sie auch das nachfolgende Faxformular ausfüllen, ausschneiden oder kopieren und mit Ihrer Bestellung an folgende Nummer faxen: [+41 44 838 31 12](tel:+41448383112)

Mitglieder der Fachverbände ISSA, ISACA, Infosurance, ASIS, SwissICT, ISSS und BCM.net/BCI sowie Hochschulangehörige und Lehrpersonal erhalten einen Rabatt von 15% auf den Studienpreis. Bitte Fachverband oder Organisation bei der Bestellung angeben.

Faxformular



ISPIN AG ZURICH | Grindelstrasse 15 | CH-8303 Bassersdorf | Switzerland | Fax: +41 44 838 31 12

ABSENDER:

Firma.....
Name.....
Vorname.....
Funktion.....
Strasse.....
PLZ/Ort.....
E-Mail.....
Tel.....
Mobil.....
Fachverband/Organisation.....

LIEFERANSCHRIFT (falls vom Absender abweichend):

Firma.....
Name.....
Vorname.....
Funktion.....
Strasse.....
PLZ/Ort.....
E-Mail.....
Tel.....
Mobil.....

BESTELLUNG

Anzahl Studien * bei 3 oder mehr Ex. erhalten Sie 15% Rabatt

Datum, Ort/Unterschrift

ISPIN AG ZURICH
swiss made security.®

Herausgeber und Kontakt

Herausgeber

ISPIN AG ZURICH . Grindelstrasse 15 . CH-8303 Bassersdorf . Switzerland
Tel.: +41 44 838 31 11 . Fax: +41 44 838 31 12 . <http://www.ispin.ch>

© ISPIN AG ZURICH 2011

Die Inhalte der Studie dürfen ausschliesslich auszugsweise und unter Nennung der ISPIN AG ZURICH zitiert werden.

An der Studie haben mitgewirkt

Marco MARCHESI, CEO der ISPIN AG ZURICH.

Marcus BEYER, Senior Architect Security Awareness bei der ISPIN AG ZURICH

Daniel STÄDELI, Senior Information Risk und Security Consultant bei der ISPIN AG ZURICH

Ivan ALLEMANN, Head Business Security und Compliance bei der ISPIN AG ZURICH

Zrinka MASLIC, Chief Technology Officer bei der ISPIN AG ZURICH

Thomas MÜLLER, Security Consultant bei der ISPIN AG ZURICH

Katja DÖRLEMANN, Assistenz Business Security bei der ISPIN AG ZURICH

Produktion

Carina LINNEMANN (Infografiken), Dietmar POKOYSKI (Fachlektorat, Layout) / known_sense (Köln)



Katja Dörlemann



Marcus Beyer

Kontakt

Katja Dörlemann/Marcus Beyer, Studienteam SecurityRadar 2011
securityradar@ispin.ch

ISPIN AG ZURICH
swiss made security.®

Themenübersicht des SecurityRadar 2011 – das erwartet Sie in diesem Studienband:

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



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