WEKA

MANAGEMENT DOSSIER

Juni 2013 – Nr. 43

VERWALTUNGSRAT

Beste Verwaltungsrats-Praxis kombiniert mit VR-Tools.

Bedrohungen aus dem Internet

Der Verwaltungsrat muss die Cyber-Abwehrschlacht steuern

Impressum

MANAGEMENT DOSSIER – Juni 2013 – Nr. 43
VERWALTUNGSRAT

Layout/Satz:	Tonio Schelker
Korrektorat:	Urs Bochsler
Druck:	Rankwoog-Print GmbH, Zofingen
Herausgeber:	Silvan Felder, Verwaltungsrat Management AG
Verlag:	WEKA Business Media AG Hermetschloostrasse 77, 8048 Zürich Telefon 044 434 88 34, Fax 044 434 89 99, info@weka.ch, www.weka.ch
Aktuelle Ausgabe:	Juni 2013
Erstausgabe:	Juni 2006
Erscheinungsweise:	Zweimonatlich

VLB – Titelaufnahme im Verzeichnis Lieferbarer Bücher:
Halbjahresabo: ISBN 978-3-297-46800-5
Jahresabo: ISBN 978-3-297-46900-2

Inhalt

Vorbemerkung: *Im Beitrag wird aus Gründen der sprachlichen Einfachheit nur die männliche Form gebraucht.*

Vorwort

Wussten Sie, dass die grösste Zahl von Cyberangriffen nicht gegen grosse sondern gegen mittlere und kleine Unternehmen und deren Daten geführt wird? Auch meine Wahrnehmung war bis anhin so, dass vor allem grosse Firmen betroffen seien. Jedoch musste ich diese bei der Lektüre des vorliegenden Management Dossiers Verwaltungsrat klar revidieren. Zugleich erkannte ich, dass CyberCrime zu einem zentralen Thema auf der Topebene der Unternehmung werden muss. Es geht dabei nicht nur um Image und Reputation. Cyber-Attacken können gar über Sein oder Nichtsein der Unternehmung in der Zukunft bestimmen. Höchste Zeit also, dass wir uns auch im Verwaltungsrat dazu Gedanken machen!

Und nun noch etwas in eigener Sache: Mit dieser Ausgabe geht nach sieben spannenden Jahren des Aufbaus und der Etablierung dieser Fachzeitschrift meine Funktion als Herausgeber zu Ende. Ich habe mich bereits im Sommer 2012 entschieden, diese Verantwortung auf den jetzigen Zeitpunkt hin an andere Personen zu übertragen.

Ich hoffe, Sie hatten mit den nun bereits 43 erschienen Ausgaben dieses Dossiers ebenso viel Spass wie ich. Und wenn auch Sie den einen oder anderen Input für Ihre VR-Arbeit und -Organisation aufnehmen konnten, so sehe ich eines meiner grundsätzlichsten Anliegen schon bestens erfüllt.

Ich möchte Ihnen liebe Leserinnen und Leser ganz herzlich für Ihre Treue über all die Jahre danken. Ebenso geht ein grosses Dankeschön an die WEKA Business Media AG. Die Besitzerin und Verlegerin dieser Schriftenreihe hat dieses erfolgreiche Projekt überhaupt erst ermöglicht und mich über all die Jahre tatkräftig unterstützt und begleitet.

Ein letztes Mal wünsche ich Ihnen unter meiner Verantwortung viel Spass bei der Lektüre.

Herzlichst Ihr Silvan Felder

Autoren dieser Ausgabe

Armin Gutmann,
Leiter Schadenversicherungen
GWP Insurance Brokers AG
Hagenholzstrasse 56
CH-8050 Zürich
armin.gutmann@gwp.ch

Philipp Pellizzaro,
Senior Broker Special Lines & International Business
GWP Insurance Brokers AG
Hagenholzstrasse 56
CH-8050 Zürich
philipp.pellizzaro@gwp.ch

Einleitung

Der Gegenwert der Betrügereien übers Internet wird jährlich auf mehrere Hundert Milliarden Dollar geschätzt. Täglich werden 150 000 Computer mit einem Virus infiziert und viele Systeme gehackt. Im tobenden weltweiten Cyberkrieg gilt für alle Verwaltungsräte: Sie sind verantwortlich für die Cybersicherheit ihres Unternehmens.

Alle Unternehmen nutzen die Möglichkeiten der Informationstechnologie und des globalen Internets. Die Steuerung der Geschäftsabwicklung, der Zahlungsverkehr, der Datenaustausch und die tägliche Kommunikation beruhen zu einem grossen Teil auf digitalen Systemen. Elektronische Kommunikationsformen über Smartphones und Soziale Medien sind mit grosser Wucht in den früher weitgehend abgeschotteten Unternehmensalltag eingedrungen. Deshalb können Unternehmen überall und jederzeit durch fahrlässige oder kriminelle Störungen des IT-Systems und Datenverluste geschädigt werden. Zur Senkung dieses Risikos sollte jedes Unternehmen die notwendigen Präventionsmassnahmen ergreifen und den Bedarf für die Versicherung der gefährlichsten Risiken abklären.

Meist ganz im Stillen sind mittlere und kleinere Unternehmen vom Cyberkrieg am meisten betroffen.

Die Medien berichten laufend über Cyber-Vorkommnisse. Der Ex-Präsident der Nationalbank Philipp Hildebrand wurde aufgrund gestohlener Kontodaten zu Fall gebracht. Auch im Steuerdauerkrieg zwischen der Schweiz und Deutschland spielen entwendete Kontodaten eine tragende Rolle. Sony hat mit der Information über den Diebstahl von mehr als hundert Millionen Kundendaten und tausenden von Musikdateien Aufsehen erregt. Der Bankgigant Citicorp musste den Raub von 360 000 Kundendatensätzen eingestehen. Der Internetchampion Google sah seinen von Millionen von Menschen genutzten E-Mail-Dienst Gmail wiederholt erfolgreich von Hackern geknackt. Nur eben: Das ist nur die spektakuläre Spitze des Eisbergs. Meist ganz im Stillen sind mittlere und kleinere Unternehmen am meisten betroffen. Deshalb müssen die Verwaltungsräte handeln und in ihrem Unternehmen für die bestmögliche Cybersicherheit sorgen.

Mögliche Haftungsfolgen für den Verwaltungsrat

Alexander Schmid ist bei epartners Rechtsanwälte in Zürich (www.epartners.ch) auf IT-Recht spezialisiert. Er hat an der Universität St.Gallen den M.A. HSG in Law und danach das Anwaltspatent des Kantons Luzern erworben. Im Gespräch mit dem «Management Dossier Verwaltungsrat» unterstreicht er: «Der Verwaltungsrat muss für eine vernünftige IT-Governance sorgen.»

Alexander Schmid, was hat der Verwaltungsrat eines Unternehmens mit der Cyberkriminalität zu tun?

Alexander Schmid: Jedes Unternehmen muss die Unternehmensinformatik vor internen und externen Angriffen sicher machen. Das ist eindeutig eine Aufgabe des Verwaltungsrats. Viele Verwaltungsräte sind sich aber oft nicht genügend bewusst, für die «IT-Governance» vollständig verantwortlich zu sein. Diese umfasst die Strukturierung und die Organisation der Unternehmensinformatik. Die Sicherheit der Unternehmensinformatik gehört auf die VR-Traktandenliste. Oft wird das vernachlässigt. Das kann für den Verwaltungsrat im Extremfall zu Haftungsfolgen führen.

Genügen in der Schweiz die Gesetzesbestimmungen zur Abschreckung von Cyberkriminalität?

Alexander Schmid: Grundsätzlich würden die geltenden gesetzlichen Bestimmungen und die Strafdrohungen bis zu einer Freiheitsstrafe von fünf Jahren genügen. Es spielen allerdings zwei Umstände hinein, die eine Verfolgung oft verhindern.

- Erstens: Es gibt zwar Straftatbestände, die vor unbefugter Datenbeschaffung schützen sollen. Dabei geht es um Tatbestände mit Bereicherungsabsicht wie Industriespionage oder ohne Bereicherungsabsicht wie Hackerangriffe. Die Anwendung dieser Straftatbestände setzt allerdings voraus, dass die jeweiligen Systeme «gegen […] unbefugten Zugriff besonders gesichert» sein müssen. Die betreffenden Systeme müssen also mit einem gewissen Schutz versehen sein. Wenn jedoch die Systeme ohne Passwörter oder einzig und allein mit den Herstellerpasswörtern eingesetzt werden, scheitert eine Verfolgung aufgrund der genannten Voraussetzungen am zu geringen Sicherheitsniveau. Das kommt bei vielen KMU leider oft vor. Um das zu verhindern, muss der Verwaltungsrat mit sinnvollen Vorgaben für den genügenden Schutz der IT sorgen.
- Zweitens: Wenn die Cyberattacken aus dem Ausland kommen, ist deren Verfolgung naturgemäss sehr schwierig. Sind Länder beteiligt, die Informatikdelikte nicht oder nicht streng ahnden, wird die Verfolgung praktisch unmöglich.

Was soll der Verwaltungsrat im Kampf gegen die Cyberkriminalität tun?

Alexander Schmid: Auf der Ebene des Verwaltungsrats fängt die Verhinderung von Cyberkriminalität mit der Festlegung einer wirksamen «IT-Governance» an. Daraus müssen sich sinnvolle Vorgaben für die Sicherung der Systeme ergeben. Zum Abwehrdispositiv gehört sicher ein zeitgemässes Alarmsystem, das vor jeglichen Angriffen warnt. Unbedingt notwendig ist auch die gezielte Verhinderung von Attacken von Innen. Dazu zählt die sorgfältige Auswahl, Sensibilisierung und Ausbildung der Mitarbeitenden, insbesondere diejenigen, die einen umfassenden Zugriff auf die IT-Systeme haben.

Alle sind potenzielle Opfer

Gunnar Porada ist ein ehemaliger Hacker. Heute berät er Unternehmen und Behörden im Bereich der IT-Sicherheit, unterstützt die Recherchen für Medienberichte, macht «Live-Hacking Vorführungen». Im Gespräch mit dem «Management Dossier Verwaltungsrat» verrät er die Regel Nummer eins der kriminellen Hacker: Möglichst unauffällig sein und die potenziellen Opfer damit einlullen.

Was sind die grössten Schwächen der Unternehmen im Kampf gegen die Cyberkriminalität?
Gunnar Porada: In der IT-Security Branche haben wir die fatale Situation, dass wir grösstenteils gar nicht gegen kriminelle Hacker kämpfen, sondern gegen die Unwissenheit und vor allem die Ignoranz der potenziellen Opfer. Die meisten Unternehmen versuchen, das Thema «IT-Verwundbarkeit und IT-Unsicherheit» komplett zu verdrängen. Sie profitieren dabei von der Regel Nummer eins, die kriminelle Hacker haben: Möglichst unauffällig sein! Wenn das Opfer glaubt, «es ist noch nie etwas passiert», kann der Hacker ewig weiter Schaden anrichten. Und macht es auch.

Aber alle Welt weiss doch heute, wie gross die Gefahr von Angriffen auf die IT-Systeme ist.
Gunnar Porada: Das stimmt. Gleichwohl geschieht Unglaubliches. Beispielsweise haben wir schon mehrmals Unternehmen und Behörden über schwerwiegende Schwachstellen in deren IT-Systemen unbeauftragt informiert und sind dabei auf Ablehnung oder sogar Widerspruch gestossen. Selbst wenn wir die Sicherheitsbehörden zur Unterstützung eingeschaltet haben, wurde das Thema bei den Opfern weiter ignoriert. Zuweilen lasen wir dann einige Zeit später in den Medien über Sicherheitsvorfälle bei den Betroffenen. Diese wären vermeidbar gewesen.

Schwachstellen erkennen und beseitigen!

Was muss getan werden?
Gunnar Porada: Die Verwaltungsräte und die Geschäftsführung müssen in ihren Unternehmen im Hinblick auf die Cyberkriminalität zu ihrem eigenen Schutz eine andere Kultur einführen. Es ist keine Schande, Schwachstellen zu haben und zu entdecken. Verwerflich ist es aber, wenn die oberste Unternehmensführung die Schwachstellen ohne Gegenmassnahmen duldet.

Hat man dann überhaupt eine Chance gegen das Heer von potenziellen Angreifern?
Gunnar Porada: Im eigentlichen Kampf gegen die Grosszahl von möglichen Angreifern im Internet haben einzelne Unternehmen nur eine kleine Chance. Google zum Beispiel hat das erkannt und bezahlt für jede gemeldete Schwachstelle Geld. Damit bindet der Internetgigant das weltweit im Netz vorhandene Know-how zur Abwehr von Angriffen grossflächig an sich. Das ist der richtige Weg: Jede Art von Hilfestellung nutzen, auch wenn sie ungefragt erfolgt.

Wie beurteilen Sie die Schweizer Gesetzgebung gegen die Cyberkriminalität?
Gunnar Porada: Im Bereich des Internets gilt grundsätzlich: Gesetze enden meist an der Landesgrenze. Zudem werden in verschiedenen Ländern die gleichen Tatbestände anders geahndet oder sind hier und dort sogar legal. Auf der andern Seite ist das Internet wirklich global. Dadurch haben es Angreifer leicht, aus der Ferne zu handeln. Selbst wenn es die bereits diskutierten weltweit geltenden Gesetze gäbe, blieben viele Angreifer nur schwer zu fassen. Schlimmer noch, geübte Hacker vermögen ihre Spuren gezielt anderen Menschen zuzuordnen. Dadurch können unschuldige Opfer, deren Identität missbraucht wird, zu Beschuldigten werden. Und sie haben aus technischer Sicht oft kaum die Möglichkeit, ihre Unschuld zu beweisen.

Sicherheit lässt sich nicht delegieren

Was halten sie denn von neuen Gesetzen und der Überwachung des Internets?

Gunnar Porada: Mit vielen Gesetzen wie beispielsweise den Bestimmungen über die SwissID und mit den Überwachungen des Internets machen wir es nur noch schlimmer. Denn wir vertrauen dann den Daten im Internet noch mehr und machen sie teilweise zu Beweisen. Dies, obwohl diese Daten nach wie vor spurlos manipulierbar sind. Das lässt sich mit «Live-Hacking Vorführungen» sehr schön aufzeigen. Wer solche Zusammenhänge klipp und klar sichtbar macht, hat nicht nur Freunde. Obwohl alle Nutzerinnen und Nutzer des Internets trotz aller Gesetze und Überwachungen potenzielle Opfer der Cyberkriminalität bleiben.

Geben Sie zum Schluss einige praktische Tipps, wie Unternehmen Cyberkriminalität verhindern können.

Gunnar Porada: IT-Sicherheit lässt sich schwer bis gar nicht delegieren. Die Tatsache, dass viele Verwaltungsräte und Geschäftsleitungsmitglieder über einen geringen technischen Sachverstand verfügen, sorgt allerdings in vielen Unternehmen für eine Kette von Fehlentscheidungen. Es ist jedem Entscheidträger zu raten, der IT-Sicherheit einen grossen Stellenwert beizumessen. Und im Hinblick auf die notwendige Entscheide vielleicht auch mal mit Mitarbeitenden an der Basis darüber zureden. In der Regel kennen «die unten» die Schwächen der IT-Systeme ganz genau. Sie werden aber oft nicht gehört und machen wegen des überall herrschenden Kostendrucks auch keine «teuren» Vorschläge. Daraus entsteht eine Frustration der Mitarbeitenden und eine Vernachlässigung des Abwehrwillens. Viele Unternehmen befinden sich deshalb im Kampf gegen die Cyberkriminalität auf einem Blindflug. Dies, bis es knallt und die Schäden zuweilen ausserhalb der Vorstellungskraft liegen. Deshalb gilt: Alle Unternehmen sollten eine vom Verwaltungsrat geführte durchdachte Politik der IT-Sicherheit betreiben. Das minimiert die potenziellen Schäden.

EIN EHEMALIGER HACKER

Der Ex-Hacker Gunnar Porada war in seiner Jugend tatsächlich als Hacker aktiv. Obwohl es damals mangels Rechtsprechung noch nicht illegal war, hat er rechtzeitig mit 19 Jahren aus Überzeugung die Seite gewechselt. Seitdem unterstützt der heute 38-Jährige Unternehmen und Behörden im Kampf gegen Cyberkriminalität. Er ist alleiniger Inhaber der innoSec GmbH in Walchwil (www.innosec.eu). Bekannt wurde er durch seine Vorträge zum Thema «Live-Hacking» und seine Berichterstattungen in internationalen Medien. So zeigte er beispielsweise im deutsche ZDF-Magazin «WISO» und der ZDF-Nachrichtensendung «Heute» Angriffsmöglichkeiten auf den elektronischen Reisepass auf. Zudem äusserte er in den Medien seine Sicherheitsbedenken zum neuen deutschen Personalausweis (nPA) und der SwissID und beschrieb die Angriffsmöglichkeiten beim gängigen Online-Bankingverfahren. Die innoSec GmbH führt international IT-Sicherheitsprüfungen (Penetrationstests) für Unternehmen und Behörden durch und berät bei IT-Sicherheitsfragen.

Cyberkriminalität im Vormarsch

Cyberkriminalität ist nach der Vermögensveruntreuung das zweithäufigste Delikt der Wirtschaftskriminalität. Rund ein Fünftel der Unternehmen sind davon betroffen. Tendenz rasch steigend. Das ist ein Befund des letzten «Global Economic Crime Survey – Swiss Edition» von PricewaterhouseCoopers. Als Cyberkriminalität werden alle Delikte bezeichnet, die mittels Computer und Internet verübt werden.

Die neuen Risiken rund um die weltweit eingesetzten elektronischen Systeme zur Geschäftsabwicklung, der Bezahlung übers Internet, des Datenaustauschs sowie der täglichen Kommunikation machen jedes Unternehmen aus allen Branchen für Cyberattacken verwundbar. Die Risiken sind auch dadurch gestiegen, weil die früher eher ethisch und «sportlich» motivierte Kriminalität von jungen Hackern in den letzten Jahren einer finanziell motivierten professionellen und häufig mafiösen Cyberkriminalität gewichen ist. Dass praktisch alle Unternehmen erheblich gefährdet sind, zeigt die folgende Aufzählung von Risiko- und Schadenquellen:

- Elektronische Verwaltung, Speicherung, Verarbeitung und Übermittlung von vertraulichen oder geheimen personenbezogenen oder geschäftsbezogenen Daten;
- Die aufgrund von gesetzlichen Vorschriften oder zur Verhinderung von Reputationsschäden beruhende Verpflichtung, die Kunden im Falle eines Abhandenkommens von sensiblen Daten zu informieren;
- Elektronische Veröffentlichung von Informationen über übliche Internetkanäle und Soziale Medien;
- Betriebsunterbrüche aufgrund von Cyberattacken;
- Erpressungshandlungen von Cyberkriminellen im Rahmen von Cyberattacken;
- Onlinegeschäfte tätigen oder sonst über das Internet Waren oder Dienstleistungen verkaufen;
- Zentrale Abspeicherung von medizinischen Informationen über die einzelnen Patienten (E-health Suisse);
- Beschädigung oder Zerstörung von Geschäftsdaten, Geschäftsgeheimnissen und Schutzrechten;
- Existenz eines leistungsfähigen Sekundärmarkts für gestohlene Kreditkarteninformationen: Erfolgreiche Hacker können sich einfach finanzieren.

Von aussen und von innen

Viele Verwaltungsräte und Geschäftsleitungen glauben, die Gefahr der Cyberkriminalität komme überwiegend aus der grossen weiten Welt von aussen. Gefürchtet werden namentlich die gezielten Angriffe von global tätigen Cyberkriminellen, von korrupten Mitbewerbern oder von beauftragten Cyber-Wirtschaftsspionage-Unternehmen. Unterschätzt wird gemäss der Wirtschaftskriminalitätsumfrage von PricewaterhouseCoopers der potenzielle Täter von innen. Das sind oft «einsame Wölfe», die aufgrund ihrer Funktion leicht Zugriff zu sensiblen Daten haben. Sie verfolgen finanzielle Ziele, wollen dem Unternehmen aus irgendwelchen Gründen bewusst schaden oder werden von aussen motiviert, wie in der Schweiz der Fall des zurückgetretenen Notenbankpräsidenten Phillip Hildebrand spektakulär aufgezeigt hat.

«Eines ist sicher: Die steigende Gefahr der Cyberkriminalität betrifft das ganze Unternehmen. Deren Abwehr darf nicht vom Verwaltungsrat weitgehend ignoriert und stillschweigend an die IT-Abteilung delegiert werden.»

Medien beachten spektakuläre Cyberangriffe, aber betroffen sind vor allem KMU

Schlag auf Schlag berichten die Medien über spektakuläre Cyberangriffe auf Regierungsstellen und Grossunternehmen. Gemäss Studien sind aber die mittleren und kleinen Unternehmen am meisten betroffen. Wichtig zu wissen für Verwaltungsräte und Geschäftsführungen: Cyberangreifer wählen gerne KMU als Zielscheibe, weil dort die Informationssicherheit häufig zu wenig ernst genommen wird.

Global verbreitete Schlagzeile anfangs Februar 2013: «Chinesische Hacker spionierten [New York Times] aus». Der Grund: Die weltweit beachtete Zeitung hat aufgrund von intensiven Recherchen berichtet, die Familie des chinesischen Ministerpräsidenten Wen Jiabao habe ein Vermögen von mehr als 2,7 Milliarden Dollar angehäuft. Dazu meinen Cyberspezialisten: «China führt mit den modernsten Cyberangriffswaffen eine Spionagekampagne gegen alle wichtigen Medienhäuser, die kritisch über China berichten.»

LinkedIn, Amazon, Yahoo, Twitter

Spektakulär sind auch die gelungenen Cyberangriffe auf bekannte Internetunternehmen. So wurden beim Online-Berufsnetzwerk LinkedIn die Passwörter von über sechs Millionen Nutzerinnen und Nutzern erfolgreich gehackt. Bei der Amazon Tochter Zappos haben sich Unbekannte Zugriff auf die persönlichen Daten von rund 24 Millionen registrierten US-Kunden verschafft. Beim Kreditkartenverarbeiter Global Payments wurden 1,5 Millionen Kreditkartendatensätze gestohlen und dann schlagartig eingesetzt. Bei Yahoo erbeuteten Hacker 450 000 Benutzernamen samt Passwörtern. Und bei Twitter hat eine Hackergruppe offenbar zum Spass mehr als 50 000 Benutzernamen und Passwörter ins Netz gestellt. All das zeigt: Die Angriffswaffen der globalen Cyberkriminellen sind den besten Abwehrsystemen ebenbürtig.

Gefahr für alle Unternehmen

Diese Fälle sind nur die Spitze des Eisbergs einer gewaltigen Gefahr für die gesamte Wirtschaft. Denn die grösste Zahl der Cyberangriffe richtet sich gegen mittlere und kleine Unternehmen und deren Daten. Der Grund: Wegen der Entwicklung der Informationstechnik findet weltweit eine immer dichter werdende Vernetzung und Datenübermittlung statt. Elektronische Kommunikationsformen wie die Sozialen Medien und die Smartphones dringen in den Unternehmensalltag ein. Deshalb können Unternehmen heute jederzeit von Cyberkriminalität geschädigt werden. Dabei brauchen die Täter nie einen Fuss auf das Unternehmensgelände zu setzen. Die Kriminellen im Netz haben die Möglichkeit, sich über die vielen Kanäle des Internets Zugang zu den Netzwerken der Unternehmen zu verschaffen. Auf diese Weise können sie sensible Unternehmensdaten vom andern Ende der Welt stehlen, verändern, beschädigen, zerstören oder ausspähen. Speziell gefährdet sind Betriebs- und Geschäftsgeheimnisse, wertvolle Fertigungstechnologien, Schutzrechte wie Patente und Lizenzen sowie Kreditkarteninformationen. Sobald diese Daten in den Besitz der Konkurrenz gelangen, kann das für das geschädigte Unternehmen höchst unangenehme Folgen haben.

Der Verwaltungsrat muss handeln

Aufgrund des hohen Schadenpotenzials und der steigenden Kapazität der Cyberkriminellen zur Schadenverursachung lautet die Regel für jeden Verwaltungsrat: Das Unternehmen muss sich bestmöglich auf die Gefahr einer Cyberattacke vorbereiten. Es genügt nicht, die notwendigen Massnahmen nach dem ersten Ernstfall zu ergreifen. «Jetzt von [reaktiv] auf [proaktiv] umsteigen», lautet die Devise.

Die Kosten für die Cybersicherheit sind einigermassen berechenbar. Die möglichen Schäden sowie die Wahrscheinlichkeit eines Schadenfalls sind aber nur schwer in Zahlen zu fassen. Deshalb ist es schwierig, im Bereich der Cybersicherheit eine saubere Wirtschaftlichkeitsrechnung zu erstellen. Gleichwohl besteht Handlungszwang.

Cyberprävention ernst nehmen

Vorab muss die Cyberprävention ernst genommen werden. Ab sofort ist die Ausrichtung der gesamten Unternehmensorganisation auf mögliche Cyberattacken Sache des Verwaltungsrats. Der Informationstechnologieverantwortliche und der Sicherheitsverantwortliche sind und bleiben in dieser Angelegenheit zwar die Berater der Verantwortungsträger. Die wichtigsten Entscheide werden aber vom obersten Unternehmensgremium gefällt. Die Umsetzung wird von diesen regelmässig überwacht. Und falls, wie das oft der Fall ist, im breiten Spektrum der Cyberprävention nicht genug internes Knowhow vorhanden ist, werden dafür externe Berater beigezogen.

Dynamische Passwortsysteme

Zur umfassenden Cyberprävention gehören einige selbstverständliche Massnahmen. Das gesamte informationstechnologische System des Unternehmens muss durch den Einsatz der jeweiligen State-of-the-art-Technologie vor Attacken geschützt werden. Dafür gibt es Konzepte, die individuell auf jedes Unternehmen angewandt werden können. Zu diesen gehören zeitgemässe Zugriffsregelungen und dynamische Passwortsysteme, regelmässige Updates, Backups, Firewalls und Antivirussyteme. Cyberattacken müssen sofort erkannt und neutralisiert werden können.

Forensische Spezialmethoden

Das Vorgehen für die interne Untersuchung einer Cyberattacke muss genau festgelegt sein. Zu diesem Zweck sollte der Einsatz von modernen kriminalistischen Untersuchungsmethoden vorbereitet sein. Denn es genügt nicht, einfach festzustellen, «es waren Hacker im System». Vielmehr muss herausgefunden werden, was kopiert, gestohlen, modifiziert oder gelöscht worden ist. Dafür braucht es «forensische» Spezialmethoden.

Mitarbeitende schulen

Für alle denkbaren Cyberattacken müssen die notwendigen Kommunikationsmassnahmen gegen innen und aussen vorbereitet werden. Dazu zählt auch die Festlegung der betrieblichen, rechtlichen und kommunikativen Sofortmassnahmen, die unmittelbar nach einer Cyberattacke eingeleitet werden sollen – und, weil sie vorbereitet sind, dann auch sofort eingeleitet werden können. Nachdem der bestmögliche technische Schutz der unternehmenseigenen Systeme realisiert ist, die Sicherheitsregeln eingeführt und die notwendigen Pläne und vorbehaltenen Entschlüsse erarbeitet sind, muss die gesamte Belegschaft über die Cyberprävention informiert werden. Für ihre besondere Cyberpräventionsaufgabe im Tagesgeschäft und im Ernstfall müssen die Mitarbeitenden gezielt geschult werden.

Mensch als Risiko

Analysen der bislang eingetretenen Fälle zeigen: Vom Mensch geht das grösste Risiko aus. Neben dem vorsätzlichen böswilligen Verhalten sind auch Unwissenheit und Fahrlässigkeit Risikofaktoren. Das zeigt beispielsweise die Verbreitung des Stuxnet-Virus, das ohne ein USB-Speichermedium kaum in die iranischen Atomanlagen hätte vordringen können. Somit gilt: Bei allen Mitarbeitenden sind das Bewusstsein für das vorhandene Cyberrisiko und eine entsprechende Verhaltensänderung erforderlich. Denn das gesunde Misstrauen aller Mitarbeitenden kann bei der Abwehr von raffinierten Cyberattacken entscheidend sein.

Zusammenarbeit mit andern Unternehmen

Bei der Zusammenarbeit mit andern Unternehmen im Bereich der Datenverarbeitung ist das gestiegene Cyberrisiko miteinzubeziehen. Beispiele dafür sind die Auslagerung der Kreditkartenabrechnung oder der Datenerfassung an andere Unternehmen - womöglich sogar im Ausland. In diesen Fällen müssen an die Partnerunternehmen die gleichen Sicherheitsanforderungen gestellt werden, wie sie im eigenen Unternehmen gelten. Das muss mit geeigneten Methoden überwacht werden. Und in den Zusammenarbeitsverträgen sind die Haftungsbestimmungen auf die Haftung im Falle einer Cyberattacke auszudehnen. Eine absolute Sicherheit gibt es nicht, aber die Risiken sind so weit wie möglich einzudämmen.

Umgang mit Sozialen Medien

In vielen Schweizer Unternehmen ist die Nutzung von Sozialen Medien wie Facebook, Twitter oder LinkedIn für die Mitarbeitenden erlaubt. Immer mehr Unternehmen setzen diese Medien sogar gezielt für ihre Unternehmenskommunikation ein. Bislang werden diese Sozialen Medien zwar noch kaum für direkte Cyberattacken missbraucht. Sie werden aber mit ausgeklügelten Methoden immer häufiger zur Massenverbreitung von Viren, Malware und zum Phishing von sensiblen Daten benutzt. Deshalb gehört zur umfassenden Cyberprävention das Monitoring und die genaue Regelung des Gebrauchs von Sozialen Medien durch die Mitarbeitenden – auch wenn dies der bisherigen Unternehmensphilosophie widerspricht.

Cyberrisiken massgeschneidert versichern

Cyberangriffe von aussen oder innen haben für jedes Unternehmen ein enormes Schadenpotenzial: Unterbruch von Betriebsabläufen, verunmöglichte Leistungen, Kosten für die Kundeninformation, Reputationsschäden, Haftpflichtansprüche von Dritten, Strafgebühren, finanzielle Verluste, Verlust von intellektuellem Eigentum, Senkung des Unternehmenswerts. Ein Teil dieser Risiken kann und sollte versichert werden.

Jedes Unternehmen muss unter der Führung des Verwaltungsrats die Risiken rund um die Cybersicherheit durch den Einsatz der State-of-the-art-Technologie und die notwendigen organisatorischen Massnahmen soweit wie möglich senken. Aber trotz aller Prävention bleiben in Bereichen wie Datenschutz, geistiges Eigentum, Ausfall der Technik, Hackerangriffen oder andern kriminellen Akten stets gewichtige Restrisiken.

«Cyber Liability Insurance»

Unter Namen wie «Cyber Liability Insurance», «Security Breach Insurance» oder «Privacy Breach Insurance» haben sich dafür namentlich in den angelsächsischen Ländern erprobte individuell einsetzbare Bausteine für Versicherungsdeckungen entwickelt. Versichert werden beispielsweise die Haftung aus der Verletzung der Privatsphäre, des Datenschutzes oder des geistigen Eigentums, die Geldstrafen von Behörden, die Haftung aufgrund von Hackeraktivitäten oder von Betriebsunterbrüchen im Onlinegeschäft oder die Beträge für Erpressungen und Belohnungen. Auch die Kosten zur Ermittlung, was denn tatsächlich gestohlen, verändert oder kopiert wurde, können mitversichert werden. Wer Niederlassungen in den USA oder England betreibt oder dort Kunden hat, muss unbedingt den Abschluss einer Versicherungsdeckung prüfen.

Deckungsbausteine einkaufen

Achtung: In der Schweiz bieten die üblichen bestehenden Policen keine umfassende Deckung für die mannigfaltigen bestehenden und neu aufkommenden Cyberrisiken. Die Deckungen müssen individuell und massgeschneidert als Bausteine zur Ergänzung der bestehenden Policen eingekauft werden. Führend sind der amerikanische und der Londoner Markt. Jetzt gibt es auch Schweizer Versicherer, welche die Cyber-Deckungskonzepte in lokale Policen umgewandelt haben. Es wird allerdings noch eine Weile dauern, bis sich hierzulande ein breiter Markt entwickelt hat.

Versicherungsbedarf analysieren

Zeitgemässe und international tätige unabhängige Versicherungsbroker bieten den Unternehmen im Bereich der Cyberrisiken einen umfassenden Service: Der individuelle Versicherungsbedarf des Unternehmens wird analysiert. Ziel: Alle Risiken erkennen, die wegen ihres Schadenpotenzials das Unternehmen erheblich beeinträchtigen könnten. Für die Risiken, die versichert werden sollen, werden die notwendigen Deckungen vermittelt. Zudem wird die Entwicklung des Problems der Haftungsrisiken rund um den dynamischen Cyberbereich und die daraus entstehende Gesetzgebung weltweit verfolgt. Von diesem Wissen können alle interessierten Unternehmen profitieren.

MELANI und KOBIK nutzen!

Verwaltungsräte und Führungskräfte von Unternehmen sowie alle Nutzerinnen und Nutzern von Computern, Smartphones und des Internets können kostenlos MELANI und KOBIK nutzen. MELANI ist die «Melde- und Analysestelle Informationssicherung des Bundes (www.melani.admin.ch)» und KOBIK die «Nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität (www.cybercrime.admin.ch)».

In der Schweiz investiert der Bund beachtlich in die Sicherheit der Informatikinfrastruktur und den Kampf gegen die Cyberkriminalität. Die Melde- und Analysestelle Informationssicherung MELANI wird vom «Informatiksteuerungsorgan des Bundes ISB (www.isb.admin.ch)» geführt. Partner sind der Nachrichtendienst des Bundes (NDB) und GovCERT.ch. Das ist das Schweizer Mitglied des «Forum of Incident Response and Security Teams FIRST», ein weltweiter Verbund von CERT-Teams aus Verwaltung, Wirtschaft und akademischen Kreisen. MELANI kann dank dieses Kooperationsmodells national und international auf den grösstmöglichen Informationspool im Bereich der Cyberbedrohungen zurückgreifen.

Berichte über Informationssicherung

MELANI richtet sich an eine offene und eine geschlossene Zielgruppe. Für alle offen ist die Internetseite www.melani.admin.ch. Die Computer- und Internetnutzer sowie namentlich die kleineren und mittleren Unternehmen können sich dort stets über die aktuellsten Gefahren und notwendigen Massnahmen im Umgang mit den Informations- und Kommunikationstechnologien informieren. In umfangreichen halbjährlichen Berichten werden regelmässig die aktuellsten Tendenzen und Entwicklungen in der weltweiten und Schweizer Informationssicherung aufgezeigt. Jedermann ist aufgerufen, mit einem einfachen Online-Meldeformular die selbst erlebten oder beobachteten Vorfälle zu melden. «Die Meldung von Fällen hilft MELANI, Trends im Internet zu erkennen und entsprechende Gegenmassnahmen zu treffen», wird der dringende Aufruf zur Mithilfe begründet.

Kritische Infrastrukturen schützen

Die geschlossene MELANI-Zielgruppe umfasst ausgewählte Betreiber von nationalen kritischen Infrastrukturen wie Energieversorger, Telekommunikationsunternehmen oder Banken. Ziel ist es, dass in diesen Bereichen Netz- und Systemunterbrechungen sowie Missbräuche selten, von kurzer Dauer, beherrschbar und von geringem Schadensausmass sind. MELANI bringt in diese Zusammenarbeit Wissen und Mittel ein, die nur einer staatlichen Stelle zur Verfügung stehen und die der Wirtschaft somit anderweitig nicht zugänglich sind.

Internetkriminalität melden

Die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK ist die zentrale Anlaufstelle für Personen, die verdächtige Internetinhalte melden möchten. Die Meldungen werden nach einer ersten Prüfung und Datensicherung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. Ausserdem durchsucht KOBIK das Internet nach Websites mit strafrechtlich relevanten Inhalten und erstellt eingehende Analysen über die Internetkriminalität.

Kampf gegen Cyberkriminelle in der Schweiz, Europa und USA

Überall wird gegen die Cyberkriminalität aufgerüstet. In der Schweiz hat der Bundesrat Mitte 2012 die «Nationale Strategie zum Schutz vor Cyberrisiken» aufgegleist. Europa hat bei der supranationalen Polizeibehörde Europol das «Europäische Zentrum zur Bekämpfung von Cyberkriminalität EC3» angesiedelt. In den USA hat Präsident Barack Obama seinem Land per Dekret mehr Cybersicherheit verordnet.

Am 27. Juni 2012 hat der Bundesrat die «Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken» gutgeheissen. Dazu soll die «Melde- und Analysestelle Informationssicherung MELANI (www.melani.admin.ch)» verstärkt werden. Mit der Strategie sollen drei Hauptziele erreicht werden:

- Die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyberbereich
- Die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen
- Die wirksame Reduktion von Cyberrisiken, insbesondere Cyberkriminalität, Cyberspionage und Cybersabotage.

Generell soll in der Schweiz unter Führung von MELANI der Informationsfluss und die gesamtheitliche Auswertung vorliegender Informationen zu Cyberrisiken und Cyberbedrohungen intensiviert und bedarfsgerechter verbreitet werden.

Europol rüstet auf

Die supranationale Polizeibehörde Europol hat 2013 den Aufbau des neuen «Europäischen Zentrums zur Bekämpfung von Cyberkriminalität EC3» gestartet. Dieses ist in Den Haag angesiedelt, wird von der Europäischen Union finanziert und umfasst im Endausbau 50 Mitarbeitende. Das Zentrum sammelt im Bereich der Cyberkriminalität europaweit Informationen und Erfahrungen, unterstützt Kriminaluntersuchungen und fördert länderübergreifende Abwehrlösungen und Aufklärungskampagnen. Zusätzlich betreibt es eine Expertengemeinschaft, um Cybercrime und Kinderpornografie wirksamer zu bekämpfen. Nationale Stellen werden gezielt ausgebildet.

Überdies wird in der Europäische Union eine neue Direktive zur Abwehr von Cyberangriffen diskutiert, die noch 2013 in Kraft treten soll. Geregelt werden sollen namentlich der Informationsaustausch über Attacken und Sicherheitslücken sowie die Verpflichtung, aufgedeckte Mängel zu beheben.

USA will mehr Cybersicherheit

US-Präsident Barack Obama hat kurz vor seiner Rede zur Lage der Nation im Februar 2013 ein Dekret unterzeichnet, das eine bessere Zusammenarbeit von privaten Unternehmen und amtlichen Stellen im Bereich der Cybersicherheit vorschreibt. Alle Beteiligten müssen zwingend die ihnen bekannten Informationen zu Angriffen und Bedrohungen untereinander austauschen. Gleichzeitig sollen Rahmenbestimmungen die Cybersicherheit jener Unternehmen besser schützen, die kritische Infrastrukturen betreiben. Laut Barack Obama beabsichtigen Feinde der USA, das Stromnetz, die Netzwerke der Finanzindustrie oder die Flugsicherung zu sabotieren. «Es darf nicht passieren, dass wir in ein paar Jahren zurückblicken und uns wundern, warum wir im Bereich der Cybersicherheit trotz der realen Bedrohungen des Staates und der Wirtschaft nichts getan haben», begründet der Präsident sein Dekret.

Die nächste Ausgabe erscheint im September 2013 in einem neuen Kleid

zum Thema

Karriereplanung auf Board & Executive-Stufe

Autor:

Christian Schaffenberger ist Global Head Board & Executive, Director Board & Executive Mercuri Urval International sowie Mitglied der Geschäftsleitung Mercuri Urval Schweiz

Seminar-Tipp

VR MANAGEMENT

SEMINAR-TIPP

WEKA-Abonnenten sparen CHF 100.–!*

Beste Verwaltungsrats-Praxis

11. Exklusives zweitägiges VR-Seminar mit Topreferenten
22. & 23. Oktober 2013, Hotel Astoria, Luzern

Infos unter www.vrmanagement.ch

*** WICHTIG:** Bitte bei Anmeldung Kundennummer angeben.

Bereits zum elften Mal führen wir unser schweizweit bestens etabliertes Verwaltungsrats-Seminar in Luzern durch. Sie gewinnen in den zwei Seminartagen einen umfassenden Überblick über ein professionelles Verwaltungsrats-Management. Sie lernen einen ganzheitlichen und methodischen Systemansatz kennen, der zur Wahrnehmung der VR-Tätigkeit und -Organisation nach besten Praxisstandards befähigt.

Der ideale Mix von Erfahrung und Kompetenz der Referenten mit eigenen VR-Tätigkeiten ist ein Garant für einen hohen Praxisbezug und Aktualität des VR-Seminars. Viel Zeit wird auch dem Erfahrungsaustausch und Networking unter den Teilnehmenden eingeräumt.

Der Teilnehmerkreis setzt sich seit Jahren aus erfahrenen wie auch angehenden Präsidenten, Delegierten und Mitgliedern von Verwaltungsräten und Stiftungsräten zusammen.

Referenten

- **Prof. Dr. Mathias Binswanger,** Professor für Volkswirtschaft und Finance an der FHNW
- **Prof. Dr. Roman Boutellier,** Professor für Technologie und Innovation ETH Zürich
- **Adrian Bult,** Profi-VR und Investor, u.a. VR-Präsident Swissgrid AG
- **Dr. Rolf Dobelli,** Unternehmer und Schriftsteller
- **Silvan Felder,** Inhaber und Geschäftsführer Verwaltungsrat Management AG
- **Andreas R. Herzog,** CFO beim Technologiekonzern Bühler AG
- **Elisabeth Meyerhans Sarasin,** Unternehmerin und Geschäftsführerin Meyerhans & Partner
- **Ines Pöschel,** Rechtsanwältin und Partnerin bei Kellerhals Anwälte
- **Georges T. Roos,** Zukunftsforscher, CEO Roos Trends & Futures

Themen

- **Best Board Practice** - Ganzheitliche und systematische VR-Tätigkeit
- **Normativ** - Der VR im gesetzlichen Rahmen
- **Strategisch** - Der VR als Gestaltungs- und Chancenrat
- **Klares Denken und Handeln** - auch ein Thema für Verwaltungsräte?
- **Risikomanagement** – Der VR im Umgang mit Risiken und Krisen
- **Personell** - Auswahl, Zusammensetzung und Organisation des VR
- **Finanzwirtschaftlich** - Der VR in der Finanzverantwortung
- **Kommunikativ** - Kommunikationspolitik in der Verantwortung des VR
- **Megatrends, Futures und Lifestyle** – Was auf Verwaltungsräte und Unternehmer zukommt

Willkommen beim sivg

Das Schweizerische Institut für Verwaltungsräte sivg ist die Plattform für amtierende und künftige Verwaltungsräte und VR-Themen. Es vernetzt branchen- und regionenübergreifend Verwaltungsräte, vermittelt ihnen Fachkompetenz, ermöglicht den direkten Erfahrungsaustausch, informiert und unterstützt.

Das sivg wurde im Sommer 2007 von erfahrenen Verwaltungsräten gegründet und richtet sich in erster Linie an praktizierende oder zukünftige Verwaltungsräte, die sich mit Fragen der strategischen Unternehmensführung auseinandersetzen. Rund 350 Mitglieder haben sich bereits eingeschrieben.

Vorteile für Mitglieder

- Aus- und Weiterbildung von VR
- Aktuelle Informationen zu VR-Themen
- Erfahrungs- und Gedankenaustausch
- VR-Zirkel
- Themenspezifische Veranstaltungen
- VR-Plattform und -Netzwerk
- Vorzugskonditionen bei Angeboten ausgewählter Partner

Die sivg-Anlässe, Veranstaltungen und Informationen sind für Mitglieder in der Regel kostenlos.

Mitgliedschaft

Die Mitgliedschaft steht allen natürlichen Personen offen, die aktuell oder zukünftig eine Verwaltungsratsfunktion ausüben. Wünschen Sie sich noch weiter zu informieren oder sind Sie interessiert an einer Mitgliedschaft? Erfahren Sie mehr über das Schweizerische Institut für Verwaltungsräte unter www.sivg.ch. Nebst weiterführenden Informationen finden Sie dort auch die Möglichkeit, sich für eine Mitgliedschaft[1] zu registrieren.

Vorstand sivg

- Peter Kofmel, Präsident
- Dominique Freymond, Vizepräsident
- Virgine Carniel
- Silvan Felder
- Dr. Stephan Hostettler
- Maja Lüscher
- Ines Pöschel

Beirat sivg

- Denis Gonseth
- Konrad Graber
- Robert E. Gubler
- Josef Inhold
- Max Kaufmann
- Arthur Loepfe
- Christophe Reymond
- Thomas Studhalter
- Peter Weigelt

sivg
Schweizerisches Institut für Verwaltungsräte

1 Der Mitgliederbeitrag beträgt CHF 500.– pro Kalenderjahr.

WEKA Business Media AG

Hermetschloostrasse 77
8048 Zürich

Tel. 044 434 88 34
Fax 044 434 89 99

info@weka.ch
www.weka.ch