KPMG

# Clarity on Cyber Security

## Cyberrisiken besser verstehen

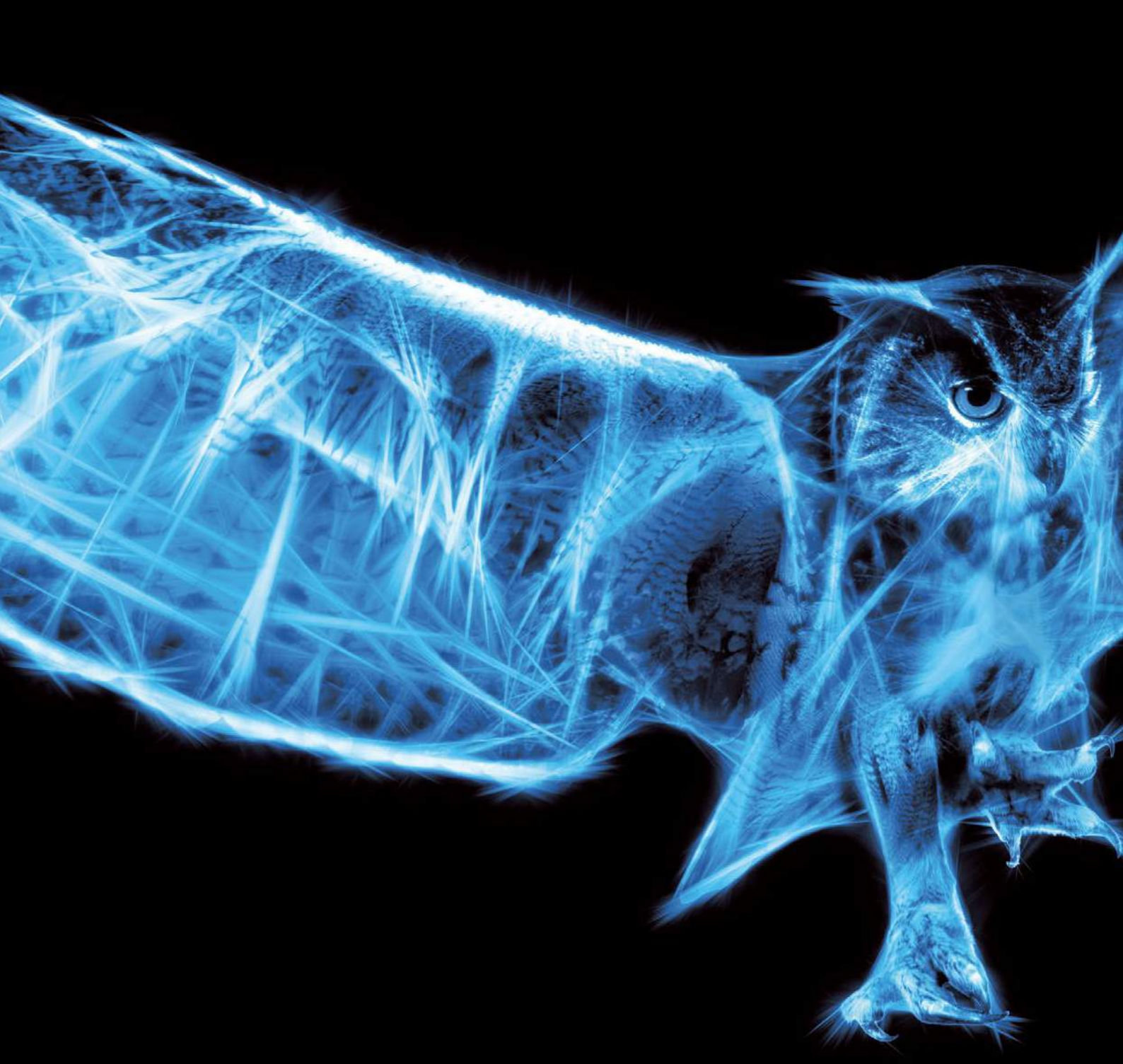
**Mai 2015**


KLARE ERKENNTNISSE
ORIENTIERUNG AN DEN GESCHÄFTS-ZIELEN
IHRE UNTER-NEHMERISCHE ZUKUNFT SICHERN
SEITE AN SEITE

INHALT

Clarity on

# Cyber Security



**AUS ANGST VOR DEN FOLGEN EINES ANGRIFFS AKTIV ZU WERDEN, FÜHRT NICHT ZUM BESTEN ERGEBNIS. EINE STRATEGIE ZUR PRÄVENTION UND REAKTION AUF CYBERATTACKEN IST DER RICHTIGE ANSATZ.**

VORWORT

**Matthias Bossardt**
Partner, Cyber Security

**Gerben Schreurs**
Partner, Cyber Security

# Cyberrisiken erkennen und verstehen

Medienberichte über Cybervorfälle gibt es heute fast täglich. Alle Organisationen und Unternehmen – ob öffentliche oder privatwirtschaftliche – scheinen extrem verwundbar angesichts der übermächtigen Stärke ihrer Angreifer – seien es Skript-Kiddies oder Vertreter einer kriminellen Organisation. Vorfälle der letzten Zeit haben erneut gezeigt, dass vor allem die Reputation eines Unternehmens auf dem Spiel steht, wenn private Informationen widerrechtlich an die Öffentlichkeit gelangen. Es versteht sich von selbst, dass Organisationen und Unternehmen ihre digitalen Vermögenswerte angemessen schützen müssen und dass ein Versagen in diesem Bereich ernsthafte Probleme nach sich ziehen kann. Cyber Security verdient deshalb einen prominenten Platz auf der Agenda des Managements.

Es ist nicht zielführend, Cyber Security nur reaktiv und aus Angst vor den Folgen eines Angriffs aktiv anzugehen. Ein besserer Ansatz ist die Erarbeitung einer wirksamen Strategie zur Prävention und zur verbesserten Reaktionsfähigkeit auf allfällige Angriffe. Das bringt uns zu der Frage: Welches ist die beste Strategie, um in einer Zeit des kontinuierlichen Wandels infolge von Digitalisierung und Globalisierung mit Bedrohungen durch Cyberkriminalität umzugehen? Und wie gehen Schweizer Unternehmen mit dieser Herausforderung konkret um?

Vor diesem Hintergrund hat KPMG eine Studie durchgeführt, an der 64 Experten für Cyber Security von Schweizer Unternehmen teilnahmen. Ergänzt wird diese Studie durch fünf Interviews mit Vertretern grosser Schweizer Unternehmen.

Das Fazit der Umfrage lautet, dass viele Organisationen und Unternehmen eine ganzheitlichere Perspektive benötigen, um sich den Herausforderungen der Cyberkriminalität wirksam stellen zu können. Dies beginnt bei einer besseren Information über die Muster dieser Bedrohungen und einem genauen Verständnis der möglichen Auswirkungen. In diesem Heft möchten wir Ihnen einen Überblick darüber geben, wie das Thema von der Geschäftswelt in der Schweiz behandelt wird – und behandelt werden sollte.

Wir hoffen, dass Ihnen die Lektüre gefällt und freuen uns darauf, Ihre Fragen persönlich mit Ihnen zu erörtern.

**Matthias Bossardt**

**Gerben Schreurs**

# DIE SITUATION IN DER SCHWEIZ

> Die Schweizer neigen dazu zu denken: Uns passiert das nicht.

Friedlich, wohlhabend und modern. Diese drei Merkmale charakterisieren die Schweiz und ihre höchst wettbewerbsfähige Wirtschaft. Seit vielen Jahren weist die Schweizer Wirtschaft eine exzellente Entwicklung auf, mit niedriger Arbeitslosenquote, hochqualifizierten Arbeitskräften und einem hohen BIP pro Kopf. Die Schweizer Wirtschaft floriert dank eines modernen Dienstleistungssektors, angeführt von der Finanzbranche sowie einer innovativen Fertigungsindustrie, die vor allem High-Tech und wissensbasierte Erzeugnisse produziert. Wirtschaftliche und politische Stabilität – sowie die Neutralität – leisten ebenso einen wichtigen Beitrag zum Image der Schweiz in puncto Vertrauenswürdigkeit. Die jüngsten Vorfälle von Cyberkriminalität stellen für den guten Ruf der Schweiz jedoch eine Bedrohung dar. Glücklicherweise ist Vertrauen aber weiterhin ein Qualitätsmerkmal der Schweiz.

Vertrauen kann sich allerdings im Zusammenhang mit Cyber Security auch als Nachteil erweisen. Wir Schweizer pflegen seit langem eine Kultur der Qualität und des Vertrauens – «wir tun, was wir sagen». Denn die Schweiz ist noch immer neutral und gilt in der Finanzwelt als sicherer Hafen. Die vorherrschende Haltung in Bezug auf Cyberkriminalität ist, dass «so etwas bei uns nicht vorkommt». Zwar ist man sich der Gefahr bewusst, doch in der Praxis erweist es sich als schwierig, dieses Bewusstsein in konkrete Massnahmen umzuwandeln.

Die Realität ist, dass für die Schweizer im Zusammenhang mit Cyber Security sehr viel auf dem Spiel steht. Für die Bankenbranche ist das Risiko sehr hoch, denn sie stellt eine attraktive Zielgruppe für direkte finanzielle Gewinne dar. Dasselbe gilt für die Schweizer Industrie und ihr geistiges Eigentum sowie ihre hohen Standards für Innovation. Die Markenzeichen des Schweizer Erfolgs sind die Qualität der Produkte – dafür steht «Swiss made» – und tief verwurzelte Werte wie Diskretion und Verschwiegenheit. Diese Markenzeichen dürften in einer stark vernetzten Welt vermehrt unter Druck geraten, wenn die Geheimnisse erfolgreicher Innovation gestohlen werden und die Vertrauenswürdigkeit in geschäftlichen Belangen ins Wanken gerät.

Weitere Schwierigkeiten können aufgrund der zunehmenden Globalisierung entstehen. Schweizer Unternehmen sind für ihre engen Verbindungen zu Unternehmen und Organisationen auf der ganzen Welt bekannt. Diese Verbindungen bergen Risiken, etwa im Outsourcing und in den Beziehungen zu Dritten. Darüber hinaus gibt es in der Schweizer Geschäftswelt zwei «Ligen»: In Unternehmen, die vornehmlich auf den Binnenmarkt ausgerichtet sind, werden die Cyberrisiken gering eingeschätzt, in internationalen Konzernen dagegen ist man sich der Risiken stärker bewusst. Insbesondere kleine und mittlere Unternehmen kennen die zunehmende Gefahr durch Cyberrisiken zu wenig.

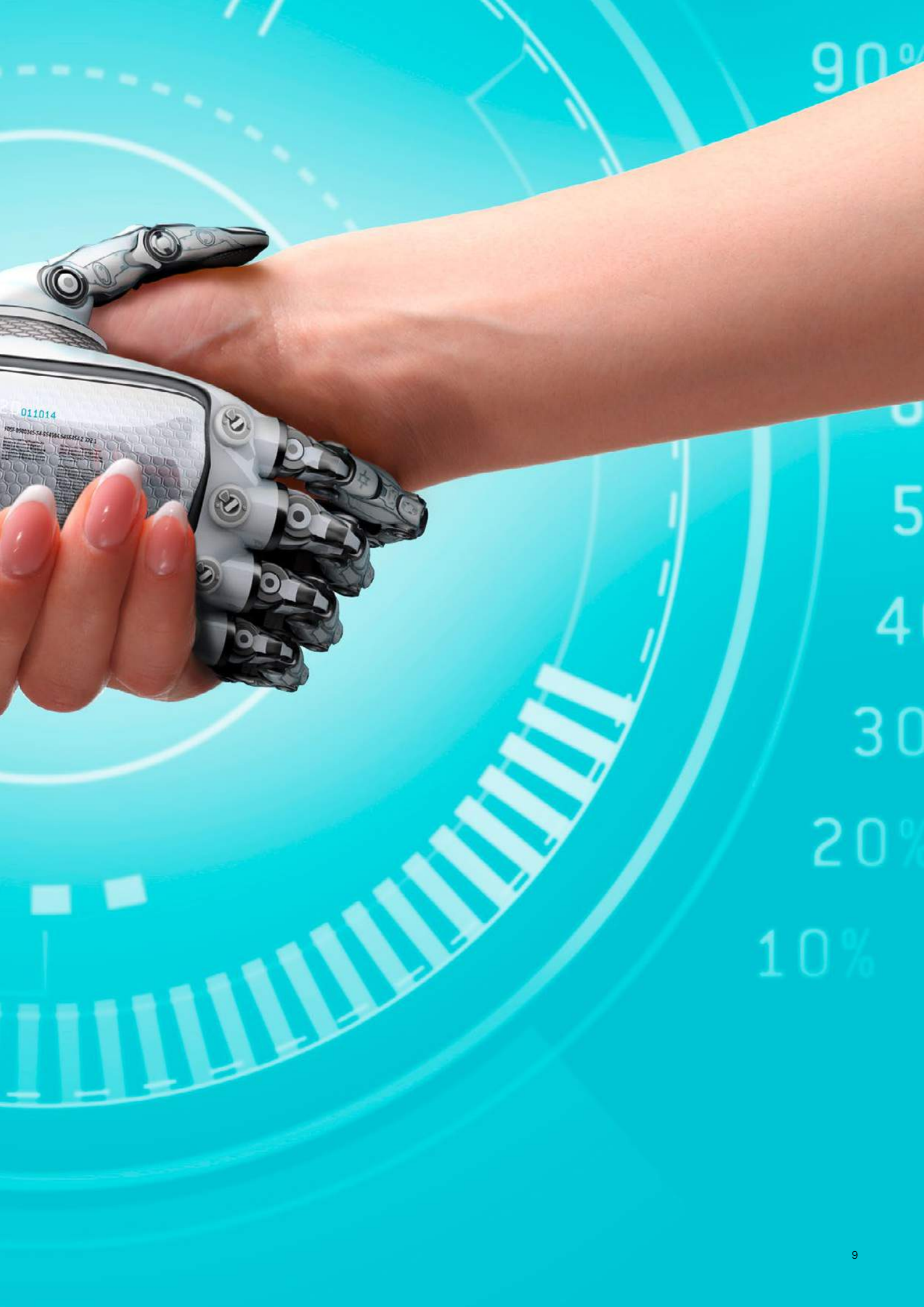
Auf den Punkt gebracht: Die Schweiz verfügt über viele attraktive Vorzüge und ist international eng vernetzt. Einige Sektoren sind heute nicht ausreichend auf das Thema Cyber Security vorbereitet. Die Kombination dieser Fakten sollte die Führungskräfte in Alarmbereitschaft versetzen.

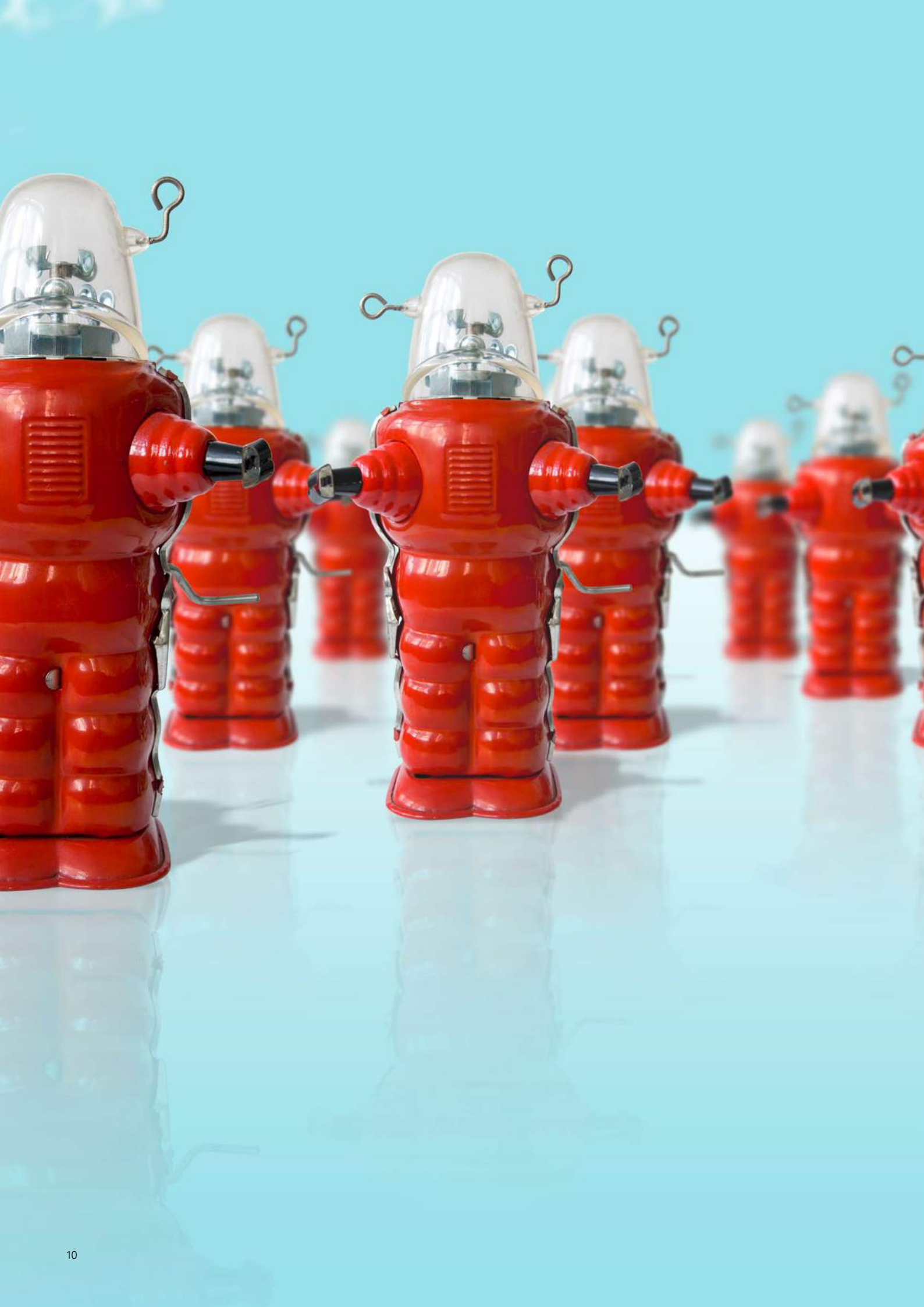
# CYBERRISIKEN VERSTEHEN

Während Cyber Security bei vielen Entscheidungsträgern weit oben auf der Agenda steht, tun sich Unternehmen schwer, genau einzuschätzen, zu messen und zu kommunizieren, inwieweit ihr Geschäft gegen Cyberangriffe gewappnet ist. Dieses Verständnis ist jedoch unabdingbar, um Cyberrisiken wirksam anzugehen.


# MENSCHEN, PROZESSE UND TECHNOLOGIE AUSGEWOGEN BERÜCK-SICHTIGEN, UM DAS RISIKO ZU MINDERN

Zwar denkt man in erster Linie an «Technologie», wenn es um die wirksame Abwehr von Cyberangriffen geht. Gefragt ist jedoch ein integrierter und ausgewogener Ansatz, der Menschen und Prozesse ebenso berücksichtigt wie Technologien.


011014
90%
5
4
30
20%
10%



# VON REAKTIV ZU VORAUSSCHAUEND

Angesichts der strategischen Bedeutung von Cyber Security dürfen Cyberrisiken nicht mehr nur reaktiv gemanagt werden. Die Aufmerksamkeit seitens der Verwaltungsräte schafft den idealen Rahmen für die Entwicklung eines erkenntnisbasierten, risikoorientierten und vorbeugenden Managements von Cyberrisiken.

# HAUPTERKENNTNISSE

## MENSCHEN, PROZESSE UND TECHNOLOGIEN AUSGEWOGEN ZU BERÜCKSICHTIGEN, IST EINE NOTWENDIGKEIT

**53%**

GLAUBEN, DASS IHRE ORGANISATION EINE AKTUELLE CYBERATTACKE ERKENNEN KANN

**53%**

GEBEN AN, DASS DER VERWALTUNGSRAT CYBER SECURITY ALS TECHNISCHES PROBLEM BETRACHTET

**59%**

SIND NICHT DAVON ÜBERZEUGT ODER WISSEN NICHT, OB IHRE SERVICE PROVIDER SICH MIT DER VERTEIDIGUNG GEGEN CYBERANGRIFFE AUSKENNEN

**14%**

TESTEN IHRE REAKTIONSPLÄNE FÜR CYBERVORFÄLLE

**45%**

DER BEFRAGTEN SAGEN, DASS ES KEINEN REAKTIONSPLAN FÜR CYBERVORFÄLLE GIBT – 32% DER GROSSUNTERNEHMEN, 52% DER FINANZINSTITUTE UND 53% DER KMU (KLEINE UND MITTLERE UNTERNEHMEN)

**36%**

GLAUBEN, DASS DIE MITARBEITENDEN SICH DES CYBERRISIKOS AUSREICHEND BEWUSST SIND

## ZU WENIG EINBLICK

**44%**

DER BEFRAGTEN SAGEN, DASS DER VERWALTUNGSRAT NICHT ÜBER METHODEN VERFÜGT, UM DAS CYBERRISIKO FÜR DAS UNTERNEHMEN ZU MESSEN

**15%**

DER UNTERNEHMEN AUSSERHALB DER FINANZBRANCHE UND 25% DER FINANZINSTITUTE GEBEN AN, DASS INFOLGE VON OUTSOURCING IHR EINBLICK IN DIE CYBER SECURITY SOWIE DEREN SICHTBARKEIT UND DIE KONTROLL-MÖGLICHKEITEN ABGENOMMEN HABEN

**50%**

DER GROSSUNTERNEHMEN VERFÜGEN ÜBER KEINERLEI ERKENNTNISSE ÜBER SCHÄDEN AUS CYBERBEDROHUNGEN

## UMGANG MIT CYBERBEDROHUNGEN

**63%**

SEHEN SICH ALS ATTRAKTIVES ZIEL VON CYBERBEDROHUNGEN

**76%**

GLAUBEN, DASS CYBER SECURITY MEHR ALS EIN MODETHEMA IST, WELCHES WIEDER AN BEDEUTUNG VERLIEREN WIRD

## VON REAKTIV ZU VORAUSSCHAUEND

**51%**

GLAUBEN, DASS CYBERANGRIFFE NICHT VOLLSTÄNDIG VERMEIDBAR SIND

**75%**

DER BEFRAGTEN STIMMEN DER AUSSAGE ZU, DASS KONTROLLEN VOR ALLEM DANN VERSTÄRKT WERDEN, NACHDEM EIN VORFALL EINGETRETEN IST

**95%**

SAGEN, DASS ES MEHR ZUSAMMENARBEIT ÜBER DIE GRENZEN DES EIGENEN UNTERNEHMENS HINAUS GEBEN SOLLTE, UM CYBERKRIMINALITÄT ERFOLGREICH ABZUWEHREN

# UMGANG MIT CYBERBEDROHUNGEN

## DREI HAUPTPRIORITÄTEN

Schon oft wurde gesagt, dass Daten in einer Welt, in der alles miteinander vernetzt ist, das neue Öl sind. Das Tempo des technischen Fortschritts ist erstaunlich, und die Welt ist dank Kommunikation und Interaktion mehr denn je ein Dorf. Die klassischen Grenzen von Organisationen – und ihren Informationssystemen – werden zunehmend aufgeweicht und zugleich können Organisationen in allen Märkten nur dann erfolgreich sein, wenn sie in agilen Koalitionen mit Partnern zusammenarbeiten. Angesichts dieser Entwicklungen ist eines ganz klar: Es ist entscheidend, dass Sie die Kontrolle über Ihre Daten und Systeme haben, wenn Sie Ihre strategischen Ziele erreichen wollen.

Die Herausforderung besteht darin, dass die Risiken in diesem Bereich zunehmen. Nie war es leichter, fertige Schadsoftware zu kaufen; die starken gegenseitigen Abhängigkeiten in einer netzwerkbasierten Gesellschaft bringen eine neue Angreifbarkeit mit sich. Die Cyberkriminalität wandelt sich. Dort, wo früher Amateure am Werk waren, sind es heute erfindungsreiche kriminelle Organisationen, die gezielte Angriffe vornehmen, entweder zu Spionagezwecken oder mit dem Ziel, massive Systemausfälle zu verursachen. Daneben haben Hacktivisten Cyberkriminalität als effektives Mittel entdeckt, um ihren Anliegen Gehör zu verschaffen, indem sie vertrauliche Informationen der Öffentlichkeit zugänglich machen. Kurz: Cyberkriminalität nimmt zu – nicht nur in Zahlen, sondern auch an Raffinesse.

### ① Der mangelnde Einblick in die Thematik Cyber Security ist eine Herausforderung

Die Umfrage zeigt, dass viele Organisationen nicht über den benötigten Einblick in die Thematik verfügen, sei es über Bedrohungen von aussen oder darüber, was für ihre Organisationen auf dem Spiel steht. Für ein effizientes Risikomanagement stellt dieser Mangel ein erhebliches Hindernis dar, denn Management von Cyberrisiken beginnt mit fundierten Entscheidungen. Das Mantra «was gemessen wird, wird auch gemanagt» verdient grössere Aufmerksamkeit.

### ② Wir brauchen den Wandel von einem technologischen zu einem ausgewogeneren Ansatz, der Mitarbeitende, Technologie und Prozesse gleichermassen berücksichtigt

Die Umfrage – in Kombination mit den begleitenden Interviews – zeigt, welche Gefahren lauern, wenn Cyber Security als rein technologische Herausforderung behandelt wird. Um das Thema Cyberkriminalität wirksam anzugehen, müssen wir die menschliche Dimension stärker berücksichtigen und einen ausgewogeneren, ganzheitlichen Ansatz verfolgen. Anbieter aus dem Technologiesektor sollten das Thema Cyber Security in Unternehmen nicht dominieren.

### ③ Organisationen sollten anstreben, ihre Fähigkeiten zur Abwehr von Internetkriminalität von reaktiv auf vorausschauend umzustellen

Die Welt der Cyberkriminalität entwickelt sich in schnellem Tempo fort. Mit gut durchdachten Ansätzen können Unternehmen ihre Risiken jedoch wirkungsvoll reduzieren, indem sie diese dabei unterstützen, Bedrohungen vorausschauend zu analysieren. Der Austausch von Informationen zwischen Organisationen trägt dazu bei, dies effektiv in die Tat umsetzen zu können.

Eine detailliertere Analyse dieser Hauptpunkte finden Sie auf den nachfolgenden Seiten.

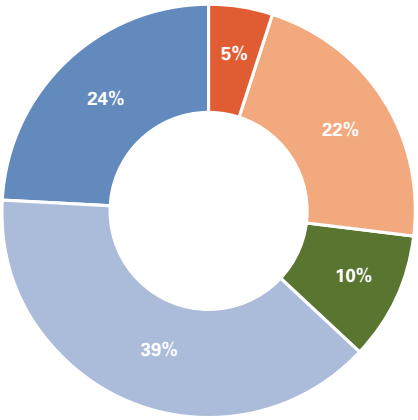
**63%**
sehen sich als attraktives Ziel von Cyberbedrohungen

**95%**
geben an, dass sie sich isoliert nicht verteidigen können

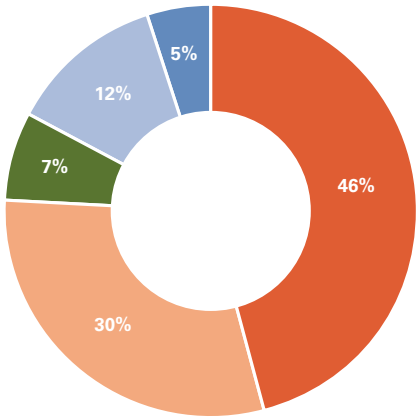
**31%**
haben Schwierigkeiten nachzuvollziehen, wie Hacker sich Zugriff auf ihre Daten verschaffen könnten

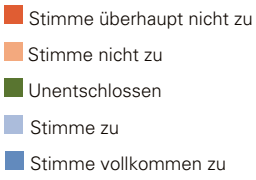
**36%**
glauben, dass die Mitarbeitenden sich des Cyberrisikos ausreichend bewusst sind

## UNSERE ORGANISATION IST EIN ATTRAKTIVES ZIEL FÜR ANGREIFER
Alle befragten Unternehmen

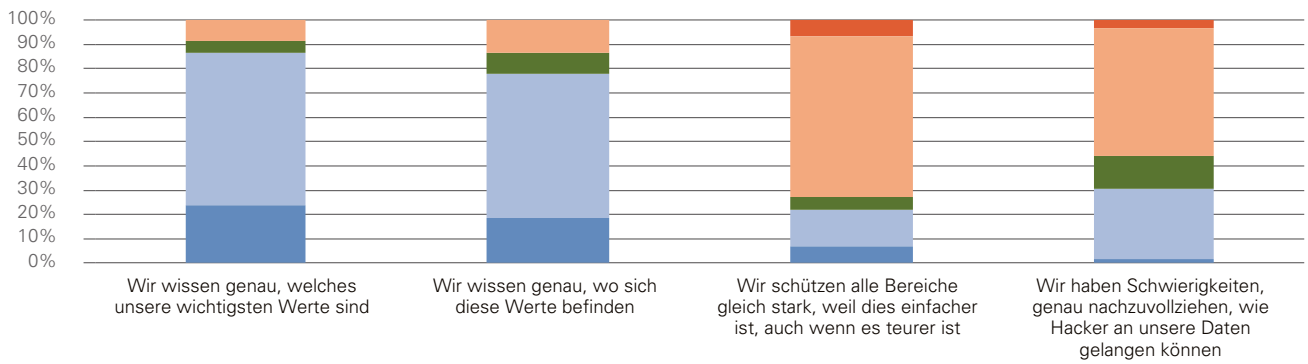



## CYBERKRIMINALITÄT IST EIN MODETHEMA OHNE BESTAND
Alle befragten Unternehmen




## MEINUNGEN ZU DER JEWEILIGEN AUSSAGE
Alle befragten Unternehmen



## INTERVIEW SWISSCOM

# EINFACHE ANWEND-BARKEIT IN DEN MITTELPUNKT STELLEN

**Was sind Ihrer Ansicht nach die derzeit grössten Herausforderungen auf dem Gebiet der Cyber Security?**
Zunächst: Diese Herausforderungen sind alles andere als neu. Sie bestehen seit vielen Jahren, und die Schwierigkeit war immer, die Einzelteile sinnvoll zusammenzusetzen. Für uns lautet eine der aktuellen Herausforderungen, eine Brücke zwischen der physischen und der Cyberwelt zu schlagen. Dies erfordert eine nahtlose Zusammenarbeit von Experten für Cyber Security auf der einen und den für Konstruktion und Installation verantwortlichen Ingenieuren auf der anderen Seite.

**Was erwarten Sie in der Zukunft? Sehen Sie bestimmte Bereiche, in denen die Bedrohungen besonders wachsen?**
Meistens können Angreifer einem der folgenden fünf Typen zugeordnet werden: der Vandale, der Kriminelle, der Hacker, der Terrorist oder die feindliche Nation. Wir könnten diese Typen weiterhin in Opportunisten und gezielte Angreifer unterteilen. Bei den opportunistischen Angriffen erwarte ich im Vergleich zu den letzten Jahren keine wesentlichen Änderungen. Meiner Ansicht nach sollten wir uns stärker um gezielte Angriffe Sorgen machen, die zunehmend professioneller werden. Die Angreifer beginnen, verschiedene Techniken miteinander zu kombinieren und erneuern auf diese Weise ihre Strategien. Zudem besteht ein wichtiger Unterschied zwischen Spionage und Sabotage. Bei der Spionage sind Muster zu erkennen, und wir können zumindest beobachten, was die Angreifer vorhaben. Bei der Sabotage jedoch, kann der Eindringling bereits strategische Plätze in Ihrem Netzwerk besetzt haben und nur auf den richtigen Moment warten, um den Schalter umzulegen. Darauf zu reagieren ist nicht leicht. Wir sollten uns zumindest bewusst machen, dass unsere Systeme wahrscheinlich schon in diesem Moment gefährdet sind. Dabei ist die eigentliche Frage nicht, ob unsere Systeme bereits gefährdet sind. Sie lautet vielmehr, wie wir damit umgehen, dass sie es sind, und wie wir die Folgen auf ein Mindestmass reduzieren können.

> Technologische Monokultur darf es in der Cyber Security nicht mehr geben. Wir müssen multidisziplinäre Daten zum Thema sammeln und uns auf den Nutzer konzentrieren.
>
> Kernaussagen von Roger Halbheer, Verantwortlicher für den Bereich Cyber Security bei Swisscom.

**Welche wesentlichen Botschaften haben Sie für Unternehmen, die wirksame Programme für Cyber Security aufbauen wollen? Und sehen Sie bestimmte Aspekte der Cyber Security, die grössere Aufmerksamkeit verdienen?**
Lassen Sie mich Ihnen drei Bereiche nennen, die im Mittelpunkt stehen sollten. Erstens sollten wir uns darauf konzentrieren, die Grundlagen für Cyber Security zu schaffen. Zweitens, und das ist sehr viel anspruchsvoller, sollten wir uns um eine einfachere Anwendbarkeit der Schutzmassnahmen für die Nutzer kümmern. Wir müssen solche Massnahmen aus der Perspektive der Nutzer und nicht aus der Perspektive der Technik betrachten. Wenn Massnahmen zu viel Arbeit verursachen oder umständlich sind, nehmen die Nutzer Sicherheitsroutinen schlichtweg nicht an. Ich sehe grosses Potenzial darin, das Smartphone als Security-Token einzusetzen, etwa zur Gesichtserkennung oder für andere einfach anzuwendende Methoden. Und drittens müssen wir unsere Angriffserkennungstechniken verbessern.

> Wir sollten beginnen, Cyber Security als etwas Alltägliches zu sehen, als Tatsache.

**Stimmt es, dass der Cyber Security Schwerpunkt heute zu sehr auf der Technologie liegt und zu wenig auf die Prozesse und Mitarbeiter abzielt?**
Einige Unternehmen für Internetsicherheit verkaufen Funktionen statt Lösungen. Daher geht es in vielen Programmen für Cyber Security vornehmlich um die Umsetzung von Tools. Dabei wird vergessen, was eigentlich nötig ist, um diese Tools zu Lösungen zu machen. Ein weiteres hartnäckiges Problem ist, dass die Angst-Strategie in diesem Bereich weiterhin vorherrschend ist. Davon wegzukommen ist schwer: Das zeigt sich schon daran, dass die Begriffe für dieses Thema überwiegend nach Krieg und Kampf klingen. Besser wäre es, Cyber Security als etwas Alltägliches zu betrachten, als Tatsache. Wie eine Erkältung, die man sich nun einmal gelegentlich einfängt, die dann etwas Aufmerksamkeit erfordert, aber auch wieder weggeht. Nicht als einen Krieg.

**Wie sehen Sie die Compliance-Regelungen für Cyber Security?**
Viele Compliance-Verfahren befassen sich damit, wie mit Vorfällen und Angriffen umzugehen ist, die wir bemerken. Diese sind jedoch nicht mein Hauptanliegen. Meine Sorge gilt eher den Bedrohungen, die nicht auf unserem Radar sind. Compliance zwingt uns dazu, die richtigen Verfahren zu befolgen und für die Vorfälle, die wir bemerken, einen Haken hinter alle richtigen Schritte zu setzen. Das kann ein extrem kontraproduktiver Reflex sein, wenn wir uns auf die eigentliche Gefahr konzentrieren müssen. Wir müssen unser Hauptaugenmerk nämlich einer besseren Datenlage zu möglichen Bedrohungen widmen und nicht einer rigoroseren Compliance.

**Sehen Sie Chancen auf eine bessere Datenlage hinsichtlich möglicher Bedrohungen?**
Absolut. Erst einmal durch eine bessere Zusammenarbeit von Organisationen, die sich ähnlichen Herausforderungen gegenüber sehen. Eine Datenbank der Beinahe-Vorfälle (Near Miss) wäre fantastisch, ist aber wohl kaum zu realisieren, wegen des Dilemmas, dass zu diesem Zweck vertrauliche Informationen zugänglich gemacht werden müssen. Davon abgesehen gibt es weitere Optionen. Wir können unsere Erkenntnisse durch die Kombination von Daten aus verschiedenen Quellen und mit Daten früherer Probleme ausbauen. Es ist wichtig, den Tunnelblick des Spezialisten zu vermeiden, daher achte ich darauf, Soziologen und Statistiker in meinem Team zu haben. Diese können ganz neue Perspektiven einbringen. Und genau das brauchen wir auf dem Gebiet der Cyber Security.


Roger Halbheer

# ZU WENIG EINBLICK
## IN DEN BEREICH CYBER SECURITY

**Auf den ersten Blick erscheinen die Ergebnisse unserer Umfrage beruhigend. Eine grosse Mehrheit von 86% der Befragten gibt an, dass ihnen vollständig bewusst ist, welche Werte sie schützen müssen. 78% geben an, dass sie ausserdem genau wissen, wo sich diese befinden.**

Unsere Erfahrung zeigt das Gegenteil und auch in einigen der von uns durchgeführten Interviews stellte sich heraus, dass sich Unternehmen schwer damit tun zu erfassen, was Cyberkriminalität für ihre Organisation wirklich bedeutet. Hier besteht eine Diskrepanz zwischen der intuitiven und der operativen Kenntnis der Werte.

Darüber hinaus haben viele Führungskräfte durch die Verwendung von technologischen Fachvokabeln Schwierigkeiten, die aktuellen Herausforderungen für das eigene Unternehmen zu erfassen. Es ist also von grosser Bedeutung, die Fachsprache der Sicherheitsindustrie zu entschlüsseln, damit man versteht, was bereits auf dem Spiel steht oder stehen könnte.

Dies spiegelt sich auch in der Tatsache wider, dass fast die Hälfte der Befragten (44%) angibt, dass der Verwaltungsrat nicht über Methoden verfügt, um das Cyberrisiko für das Geschäft zu messen. Etwas über die Hälfte (53%) gibt an, dass die Risikobereitschaft in Bezug auf Cyberkriminalität im Verwaltungsrat diskutiert wird. Dabei geht es um das geeignete Risikomanagement für die jeweilige Risikobereitschaft. Darüber hinaus scheinen Unternehmen in Bezug auf die Messung der Rendite ihrer Sicherheitsinvestitionen im Dunklen zu tappen: 39% der Befragten überwachen den Gesamtschaden (d.h. den direkten und indirekten) eines Cyberangriffs nicht.
In vielen anderen Investmentkategorien, in denen die Investitionsrendite eines der Hauptkriterien für Entscheidungsträger ist, wäre ein solcher Mangel an Informationen inakzeptabel. Unter den Grossunternehmen ist diese Zahl sogar noch höher. Dort gaben 50% der Befragten an, über keine Erkenntnisse hinsichtlich des Schadens zu verfügen. Eine mögliche Erklärung ist, dass sich die Messung der Wirkung in grösseren Unternehmen komplexer gestaltet. Insgesamt scheint die Aussage gerechtfertigt zu sein, dass es in vielen Unternehmen an den notwendigen Erkenntnissen fehlt, um fundierte Entscheidungen in Bezug auf die Cyber Security treffen zu können. IT-Verantwortliche müssen in der Lage sein, faktengestützte Investmententscheidungen zur Abwehr von Cyberrisiken zu treffen. Gelingt ihnen das, werden Entscheider für die Sache gewonnen sowie Verständnis, Vertrauen und Glaubwürdigkeit geschaffen. In der Praxis wird jedoch überwiegend reaktiv vorgegangen. Dies bildet einen starken Kontrast zu anderen Bereichen – etwa dem kaufmännischen Management. Dort sind relevante Informationen oft nur wenige Klicks entfernt, so dass strategische Entscheidungen, wie Unternehmensübernahmen oder der Eintritt in neue Marktsegmente, gerechtfertigt werden können. Es gibt keinen Grund, warum Erkenntnisse über die Cyber Security nicht in einem vergleichbaren Umfang erhältlich sein sollten. Sie sind von grosser Bedeutung: Wenn es an wirksamer Cyber Security mangelt, kann dies ernste Folgen haben und verhindern, dass Organisationen ihre strategischen Ziele erreichen.

All dies legt die Anwendung eines Risikomanagement-Ansatzes für Cyber Security nahe. Im Wesentlichen bedeutet Cyber Security die Durchführung einer Risiko-Analyse aus Sicht der Organisation sowie des Angreifers (Prävention), das Identifizieren und Analysieren kritischer Werte (Erkennung) und die Einführung einer Bereitschaftsorganisation für die Reaktion auf Vorfälle (Reaktion). Der Erfolg eines solchen Ansatzes ist allerdings von einer soliden Datenlage abhängig.

**58%**

der Befragten sagen, dass der Bereich IT-Sicherheit nicht direkt dem Verwaltungsrat berichtet

**44%**

der Verwaltungsratsmitglieder kennen die Risiken der Cyberkriminalität nicht ausreichend

**51%**

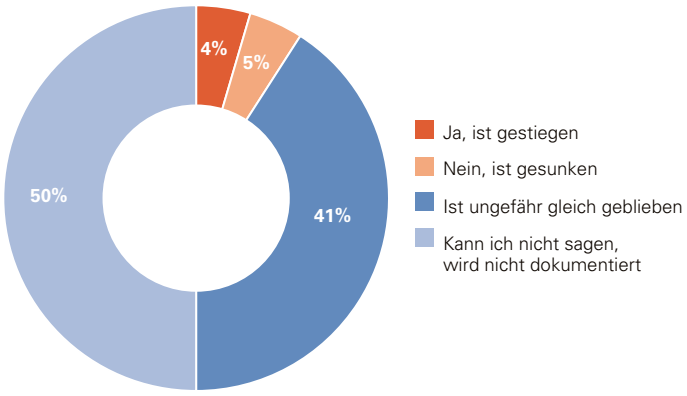
können aktuelle Angriffe nicht erkennen

**59%**

sind nicht überzeugt, dass ihre Service Provider sich mit der Abwehr von Cyberattacken auskennen

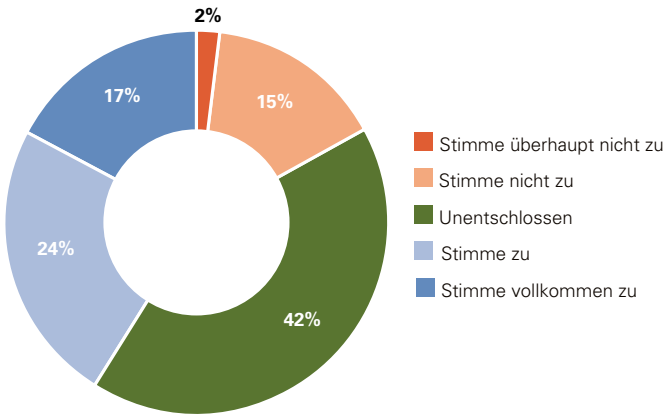
### IST DER GESAMTSCHADEN (DIREKT UND INDIREKT) GEGENÜBER DEN VORANGEGANGENEN 12 MONATEN GESTIEGEN?

Unternehmen > 5.000 FTE



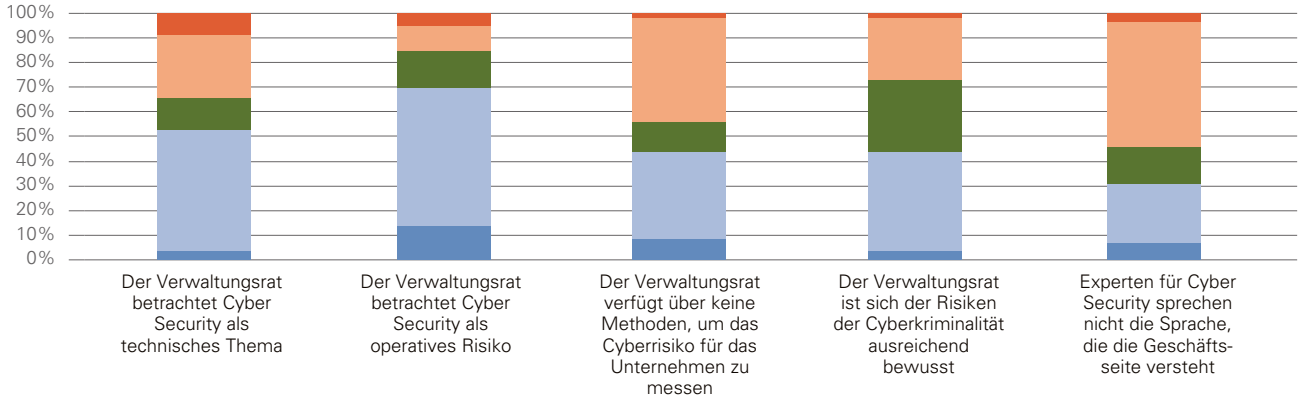

### UNSERE PROVIDER KENNEN SICH MIT DER ABWEHR VON CYBERATTACKEN AUS

Alle befragten Unternehmen




### MEINUNGEN ZU DER JEWEILIGEN AUSSAGE

Alle befragten Unternehmen



## INTERVIEW HELSANA GROUP

# DER KRANKEN-VERSICHERUNGSSEKTOR IST EINE STABILE BRANCHE

**Ist der Krankenversicherungssektor ein attraktives Ziel für Hacker?**
Meiner Erfahrung nach eigentlich nicht. Unsere Branche ist ziemlich stabil und ruhig, weil finanzielle Interessen für uns nicht im Vordergrund stehen, wie etwa im Bankensektor. Adressinformationen und Angaben zum Gesundheitszustand der Kunden, die dem Datenschutzgesetz und unserer Geheimhaltungspflicht unterliegen, könnten von Interesse sein, weil mit diesen Geld zu verdienen wäre. Darüber hinaus würden solche Vorfälle unseren Ruf schädigen. Industriespionage spielt für unseren Sektor hingegen eher eine untergeordnete Rolle, weil neue Versicherungsprodukte über Jahre entwickelt werden und daher nicht von Interesse sind.

> Der Krankenversicherungssektor ist derzeit kein attraktives Ziel für Hacker. Der Austausch zwischen Unternehmen einer Branche ist wichtig. Outsourcing und Cloud Services stellen ein Risiko dar. Die externen Anbieter verfügen heute über gute Sicherheitsmassnahmen.
>
> Kernaussagen von Stefan Burau, Verantwortlicher für Informationssicherheit bei der Helsana-Gruppe.

**Welches sind die Herausforderungen im Zusammenhang mit Cyber Security?**
Die Resilienz der Sicherheitsprozesse und die Organisation sowie Verfügbarkeit des Security Operations Center (SOC) sind unsere grössten Anliegen. Wir wollen proaktive Lösungen in den Bereichen IS Governance umsetzen und das SOC wird das Berichtswesen und die verantwortlichen Stellen festlegen.

**Viele Unternehmen beginnen erst dann in die IT zu investieren, nachdem es einen Vorfall gegeben hat. Stimmen Sie zu?**
Absolut. Meist weiss die Unternehmensleitung nicht, was auf dem Gebiet der Cyber Security vorgeht. Die Sicherheitsspezialisten werden erst dann aufgefordert zu berichten, nachdem es einen Vorfall gegeben hat. Andererseits stehen wir im regelmässigen Kontakt zum CIO und mehreren Mitgliedern des Verwaltungsrats.

**Wie wichtig ist der Austausch mit anderen Unternehmen?**
Sehr wichtig. Ein Austausch zwischen den Versicherungsgesellschaften wird bis zu vier Mal jährlich organisiert. Auf solchen Veranstaltungen sprechen wir offen über Themen der Informationssicherheit, wie Vorfälle und potenzielle Risiken. Meiner Meinung sollten solche Zusammenkünfte extern organisiert und moderiert werden.

**Können die Unternehmen die Sicherheit gewährleisten, wenn sie ihre IT-Abteilungen outsourcen?**
Es besteht immer ein Risiko. Heute nimmt die Abhängigkeit von Outsourcing und Cloud Services zu. Alle Punkte werden

im Vertrag mit dem externen Anbieter festgelegt. Wichtig ist, dass der Outsourcing- oder Cloud-Anbieter einen ausgereiften und gut dokumentierten Kontrollrahmen für IT- und IS-Governance implementiert hat. Darüber hinaus muss getestet werden, ob die Service Provider geeignete Sicherheitskontrollen eingerichtet haben, über die im vereinbarten Umfang regelmässig Berichte vorgelegt werden.

**Würden Sie ebenfalls sagen, dass in Ihrer Organisation die Compliance mehr im Vordergrund steht als die Sicherheit?**

In Bezug auf den Datenschutz und die Befolgung der Datenschutzgesetze der Schweiz stimme ich dieser Aussage zu. Andererseits aber sehe ich, dass die Themen Sicherheit und Governance in den letzten Jahren an Bedeutung zugenommen haben.

Stefan Burau

> Es gilt zu prüfen, ob Service Provider geeignete Sicherheitskontrollen eingerichtet haben.

# WIR BRAUCHEN DEN WANDEL

## VON EINEM TECHNOLOGISCHEN ZU EINEM AUSGEWOGENEREN ANSATZ, DER MITARBEITENDE, TECHNOLOGIE UND PROZESSE GLEICHERMASSEN BERÜCKSICHTIGT

**Die Hälfte der Befragten gibt an, dass ihr Verwaltungsrat Cyber Security als technisches Problem betrachtet. Zwei Drittel räumen ein, dass Cyber Security zu stark auf Technologie beruht. Daran lässt sich klar ablesen, dass den anderen zwei Säulen einer vollständigen und ausgewogenen Strategie zu wenig Aufmerksamkeit geschenkt wird: Mitarbeitenden und Prozessen.**

Dieses Ergebnis hängt eng damit zusammen, dass Cyber Security ein noch relativ junges Thema ist. Die Branche hat sich binnen kurzer Zeit entwickelt und eine Reihe von Konzepten, Tools und Techniken auf den Markt gebracht. Für Führungskräfte mag es verlockend sein, diese Lösungen zu übernehmen, um ein gutes Gewissen in Bezug auf die Sicherheit ihrer Organisation und ihre digitalen Vermögenswerte zu haben. Jeder kann Security Tools kaufen – einen ganzheitlichen Ansatz auf die Beine zu stellen, ist jedoch sehr viel anspruchsvoller.

Die Realität ist, dass Technologie nur einen Teil der Gleichung auf dem Gebiet der Cyber Security ist und ein isolierter technischer Ansatz daher ein trügerisches Sicherheitsgefühl erzeugt. Mit anderen Worten: Auch das beste Tool hilft nicht, wenn die Strategie nicht stimmt.

Organisationen sollten einen ausgewogeneren Ansatz verfolgen. Eine Strategie für Cyber Security sollte unter Einbeziehung der damit eng verknüpften Einflussfaktoren «Mitarbeitende», «Prozesse» und «Technologie» eine kostenwirksame Kontrolle des Cyberumfelds ermöglichen. Am besten gelingt dies, wenn die Nutzererfahrung – statt der Technologie – den Mittelpunkt des Cyber-Security-Ansatzes bildet. Cyber Security ist nicht gleichzusetzen mit Tools und Technologien; sie entsteht dann, wenn die Menschen diese Tools und Technologien ganz selbstverständlich nutzen, weil sie nutzerfreundlich sind. Die Fachleute im Bereich der Computersicherheit haben hier eine Verantwortung: Ihr Interesse darf nicht ausschliesslich der Technik gelten, sondern Sie brauchen auch die Fähigkeiten, dieses Thema im grösseren Zusammenhang von Menschen, Prozessen und Technologien darzustellen.

Dies bringt mit sich, dass Cyber Security nicht an spezielle Abteilungen delegierbar ist. Cyberkriminelle können nicht nur mit Hilfe ausgereifter Technologien in eine Organisation eindringen, sondern dies auch über Social Engineering versuchen oder indem sie die Sorglosigkeit von Mitarbeitenden ausnutzen. Das Sicherheitsniveau steht und fällt mit dem schwächsten Punkt in einer Organisation. Daher betrifft Cyber Security alle Mitarbeitenden in einer Organisation und sollte nicht an eine Gruppe von Spezialisten delegiert werden. Cyber Security ist eine Einstellung, keine Abteilung. Um das Bewusstsein dafür zu schaffen ist es wichtig, dass die Unternehmensleitung mit gutem Beispiel vorangeht und das Thema stärker in den Fokus rückt. Führungskräfte, die ihrem eigenen Anspruch Taten folgen lassen – indem sie etwa verlangen, dass ihre eigenen Mobilfunkgeräte und Tablets gesichert sind – haben eine grössere Wirkung auf den Rest der Organisation. Führungskräfte, die kein solches Vorbild sind, riskieren, dass auch der Rest der Organisation die Sicherheitsstandards reduziert.

**48%**

sagen, dass die Mitarbeitenden sich der Cyberrisiken nicht ausreichend bewusst sind

**61%**

finden, dass Cyber Security zu stark technologieorientiert ist

**53%**

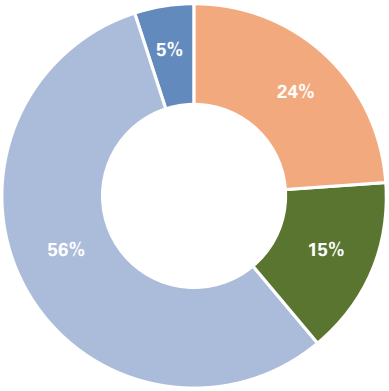
sagen, dass ihr Verwaltungsrat Cyber Security als technisches Thema betrachtet

**31%**

stimmen zu, dass Experten für Cyber Security nicht die Sprache sprechen, die das Management versteht

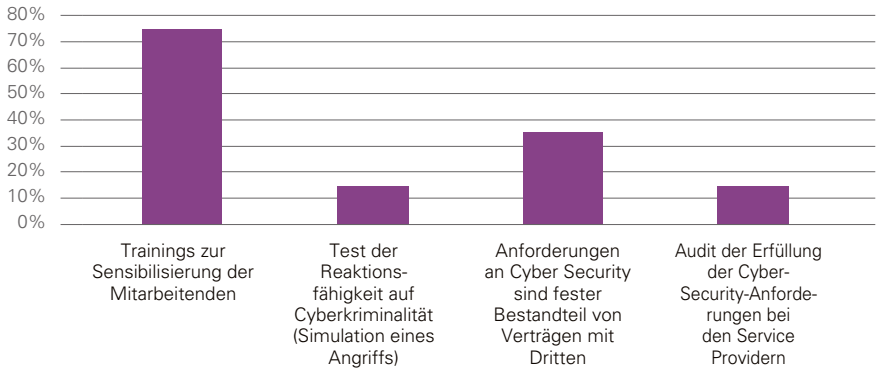
## CYBER SECURITY IST ZU STARK TECHNOLOGIEFOKUSSIERT

Alle befragten Unternehmen



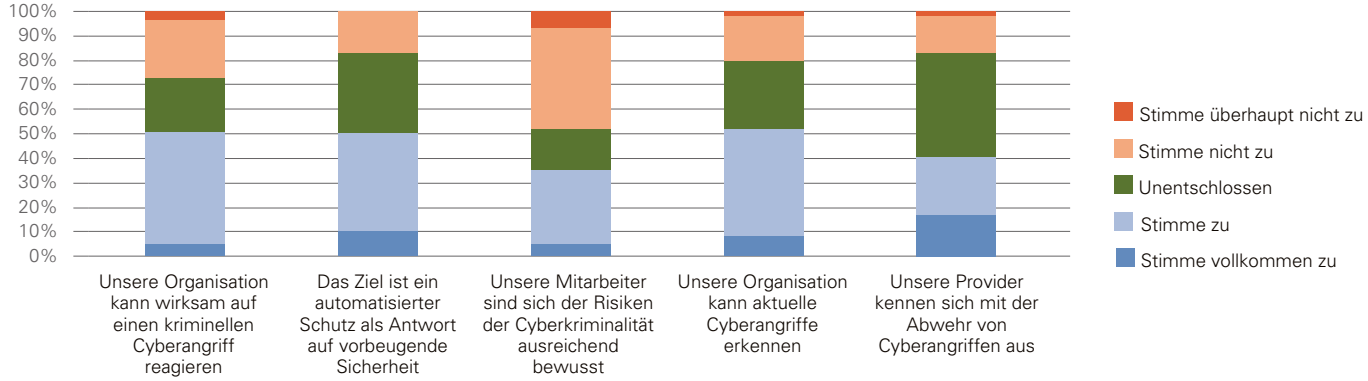

## WELCHE KONTROLLEN HABEN SIE ZUR ABWEHR VON CYBERATTACKEN EINGERICHTET?

Alle befragten Unternehmen




## MEINUNGEN ZU DER JEWEILIGEN AUSSAGE

Alle befragten Unternehmen



## INTERVIEW ALPIQ

# SICHERHEIT ALS STRATEGISCHES THEMA BEHANDELN

**Was ist ganz allgemein Ihre Meinung zu den Trends auf dem Gebiet der Cyber Security?**

Köhler: Cyber Security ist ein zunehmend wichtiges Thema und sowohl Bedrohungsszenarien als auch Angriffsmethoden werden immer komplexer. In der Vergangenheit war es möglich, sensible Daten und Systeme physisch zu isolieren. Heute sind weder eine physische noch eine elektronische Isolierung gangbare Wege. Dieser hohe Grad an Komplexität hat zu einer grösseren Angriffsfläche geführt und stellt die Unternehmen heute vor eine grosse Herausforderung: Wie können sie die Komplexität dieser Systeme bewältigen?

Meier: Heute werden viele Prozesse über die Cloud abgewickelt und in vielen Fällen wissen wir nicht, welche Art von Daten von welchen Personen angesehen werden oder wer Zugang zu diesen hat. Dies ist einer der Gründe, weshalb wir Cyber Security nicht nur auf der technischen Ebene betrachten sollten. Der menschliche Faktor stellt eine wesentliche und enorme Schwachstelle dar. Ich beobachte einen allgemeinen Mangel an Bewusstsein für den sicheren Umgang mit Informationen. Menschen geben gedankenlos Informationen an die Öffentlichkeit und schaffen so Möglichkeiten zum Beobachten und Ausspionieren. Es ist von entscheidender Bedeutung, dass die Gesellschaft sich dieser Bedrohung bewusst wird.

> Das Bewusstsein für Cyber Security ist in den letzten Jahren zwar beträchtlich gestiegen, hinkt jedoch möglicherweise der sich schnell ändernden Realität hinterher. Eine der Herausforderungen beim Aufbau einer widerstandsfähigen Organisation ist es, Cyber Security als strategisches Thema zu behandeln, statt nach Vorfällen in panikartigen Aktionismus zu verfallen.
>
> Kernaussagen von Werner Meier, Head Group Security und Urs Köhler, Information Security Officer der Alpiq AG.

**Haben Sie den Eindruck, dass Unternehmen den technischen Aspekt von Cyber Security überbewerten?**

Köhler: Sicherheit wird immer von einer Kombination aus dem menschlichen Faktor (dem Verhalten) und der Situation abhängen. Auch die Menschen sollten beobachtet werden und es sollten Kontrollen durchgeführt werden, nicht nur um Datenlecks zu verhindern, sondern auch für das Identitäts- und Zugriffsmanagement. Unternehmen werden angreifbar, wenn Mitarbeitende unzufrieden sind oder das Unternehmen unzufrieden verlassen. Manche wollen sich dann rächen. Dies stellt ein reales Risiko im breiteren Sinne dar und führt potenziell zu Sabotage oder Datendiebstahl.

Meier: In unserer Organisation unterstreichen wir die Bedeutung der menschlichen Dimension und schenken unserer Unternehmenskultur grosse Aufmerksamkeit. Wir erhöhen das Sicherheitsbewusstsein nach dem Motto «Lived by All». Sicherheit muss in den Köpfen der Leute verankert sein. Das Sicherheitsteam muss dieses Mantra entwickeln, damit jeder einzelne daran glaubt und als eigenen Wert verinnerlicht.

**Was ist die beste Strategie, um die Verwaltungsratsmitglieder in diese Thematik einzubinden?**

Meier: Mit Cyber Security werden häufig schlechte Nachrichten verknüpft, die niemand hören will und für die keiner bezahlen möchte. Damit stecken die Sicherheitsbeauftragten in einer klassischen Zwickmühle, ohne einfachen Ausweg. Sicherheit muss ein strategisches Thema sein und in der Sprache des Managements präsentiert werden – ein schwieriger Spagat. Cyber Security wird oft als Nebenthema betrachtet. Tritt jedoch dann der Ernstfall ein, fragt plötzlich jeder: «Warum hat denn niemand etwas dagegen unternommen? Wie konnte das passieren?» Und plötzlich ist


Urs Köhler


Werner Meier

Sicherheit wieder ein Hauptthema. Problematisch daran ist das Risiko potenziell panischer Reaktionen, woraufhin die Dynamik wieder abflacht, sobald die schlechten Nachrichten an Aktualität verlieren. Sicherheit als strategisches Thema zu behandeln, ist die Antwort auf dieses Dilemma.
Köhler: Die interne Revision spielt als Schnittstelle, die mit dem Verwaltungsrat kommuniziert, eine wichtige Rolle. Gepaart mit integrierter Sicherheit verhilft uns dies zu einem guten Zugang zum Verwaltungsrat. Der Prüfungs- und Risikoausschuss schenkt dem Thema die notwendige Aufmerksamkeit.

**Wie nehmen Sie das Risiko von Angriffen über Lieferanten wahr?**

Köhler: Wir betreiben bei der Auswahl unserer Partner einen erheblichen Aufwand. Wir wollen wissen, wie die Prozesse bei den Providern funktionieren und diese bewerten. Wenn es gelingt, spezifische Parameter zu definieren, erhält man eine sehr gute Qualität gepaart mit Sicherheit. Nicht nur kostengünstige Beschaffung ist wichtig, man muss die definierten Parameter auch bewerten. Es ist wahrscheinlich, dass wir nicht über alle notwendigen qualitativen Instrumente verfügen, um diese Kontrollen durchzuführen. Dennoch gibt es Möglichkeiten. In den SLAs wird dann entschieden, ob und in welchem Umfang die Anforderungen erfüllt sind. Wir können diesen Prozess überwachen und kontinuierlich verbessern. Wenn das nicht gelingt, ist der Prozess nutzlos.

> Der menschliche Faktor stellt eine wesentliche und enorme Schwachstelle dar.

# VON REAKTIV ZU VORAUSSCHAUEND

## ORGANISATIONEN MÜSSEN IHRE REAKTIONSFÄHIGKEIT AUF CYBERANGRIFFE WEITERENTWICKELN

> Vorfälle sind noch immer die häufigsten Auslöser für Investitionen in Cyber Security.

Unsere Umfrage zeigt, dass der wichtigste Auslöser (75% Zustimmung) für eine Intensivierung von Kontrollen das Eintreten eines Vorfalls ist. Dieser Reflex ist nicht sehr überraschend und ausserdem völlig verständlich. Er ist jedoch auch ein klares Zeichen, dass viele Cyberstrategien überwiegend reaktiven Charakter haben. Diese Unausgereiftheit kann auch bedeuten, dass die Organisationen sich auf die falschen Bereiche konzentrieren: So verpassen sie wahrscheinlich aufkommende Themen und werden schliesslich irgendwann von einer sich kontinuierlich verändernden Technologielandschaft überwältigt.

In diesem Zusammenhang zeigen unsere Studienergebnisse, dass Compliance bei allen Investitionen in Cyber Security ein beherrschender Faktor zu sein scheint. Knapp über die Hälfte der Befragten ist der Ansicht, dass in ihrer Organisation stärker auf Compliance als auf Sicherheit gesetzt wird. Zugleich nutzen viele Compliance, um Sicherheitsziele zu erreichen. In der Praxis sind die Unterschiede zwischen den Organisationen und Sektoren in dieser Hinsicht sehr gross. In einigen Organisationen besteht der Handlungsansatz einzig und allein aus Reaktionen auf Vorfälle und die reaktiven Investitionen im Bereich Cyber Security sind von Angst geprägt. Am anderen Ende des Spektrums befinden sich Organisationen mit sehr viel grösserem Selbstvertrauen. Durch ein kontinuierliches Scannen möglicher Bedrohungen und Analysen von Datenmustern haben sie Fähigkeiten entwickelt, anhand derer sie Charakter und Art künftiger Vorfälle vorhersagen können.

Es lassen sich grob vier Reifestufen von Organisationen in Bezug auf Cyberstrategien unterscheiden, angefangen bei reaktiven über strukturierte, integrierte bis hin zu vorausschauenden Organisationen.

Um den höchsten Reifegrad zu erzielen – der für namhafte Organisationen unabdingbar ist – müssen diese neue Wege erschliessen. Sie sollten sich selbstverständlich darauf konzentrieren, gut über mögliche Bedrohungen informiert zu sein und in eine angemessene Verteidigung investieren. Allerdings sollten sie nicht isoliert vorgehen, sondern vielmehr das Wissen und die Erfahrungen ähnlicher Organisationen aus dem öffentlichen und privatwirtschaftlichen Sektor nutzen. Eine gemeinsame Anstrengung ist entscheidend, um einen hohen Grad an Informiertheit zu erlangen. Untermauert wird dies von den Ergebnissen unserer Umfrage: Nahezu alle Befragten sind davon überzeugt, dass sie sich nicht verteidigen können, wenn sie isoliert vorgehen, und dass es mehr Kooperation geben sollte.

Ein weiterer wichtiger Aspekt ist besseres Wissensmanagement. Erkenntnisse können um intelligente Kombinationen von Daten aus verschiedenen Quellen und durch das Kombinieren von Daten mit Vorfällen aus der Vergangenheit bereichert werden. Ein multidisziplinärer Ansatz hilft, Fachblindheit zu vermeiden und bringt die notwendigen neuen Perspektiven, um die Vorhersage von Risikobereichen zu verbessern.

**37%**

sagen, dass ein Angriff auf einen Wettbewerber oder einen externen Dienstleister ein Grund für die Intensivierung von Kontrollen ist

**51%**

der Befragten sagen, dass ein Hauptgrund für die Intensivierung von Kontrollen ein gestiegenes Bewusstsein in der Unternehmensleitung ist

**75%**

der Befragten stimmen der Aussage zu, dass der wesentliche Auslöser für eine Intensivierung von Kontrollen ein Vorfall ist

**55%**

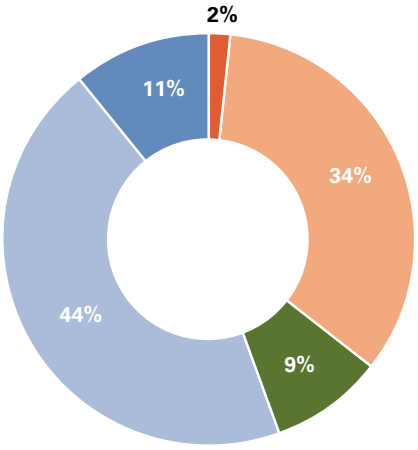
sagen, dass ihre Organisation stärker auf Compliance als auf Security setzt

**51%**

glauben, dass Cyberangriffe nicht zu verhindern sind

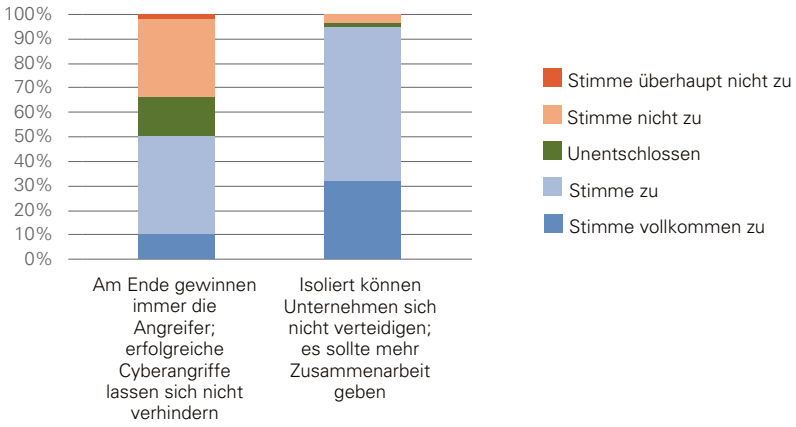
## IN UNSERER ORGANISATION WIRD MEHR WERT AUF COMPLIANCE ALS AUF SICHERHEIT GELEGT

Alle befragten Unternehmen



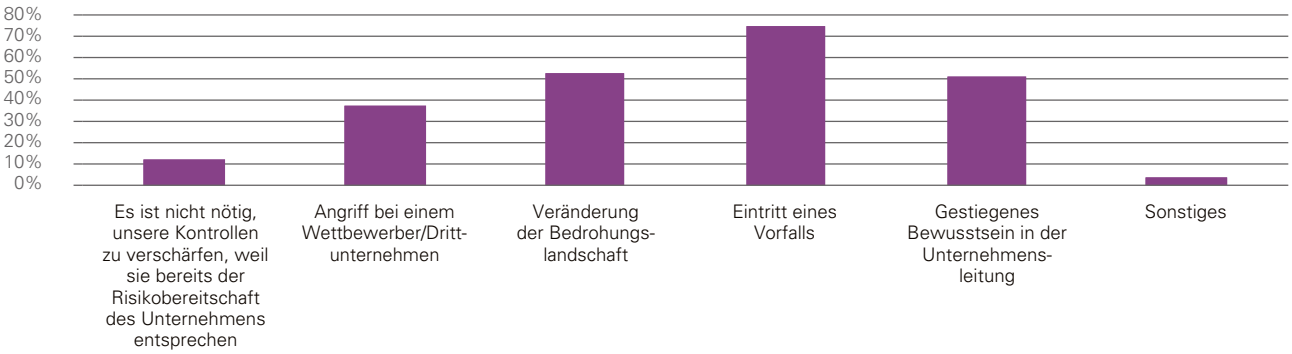

## MEINUNGEN ZU DER JEWEILIGEN AUSSAGE

Alle befragten Unternehmen




## WAS SIND IN IHRER ORGANISATION DIE AUSLÖSER DAFÜR, DASS DER VERWALTUNGSRAT DIE KONTROLLEN ZUR VERMEIDUNG VON INTERNETKRIMINALITÄT INTENSIVIERT?

Alle befragten Unternehmen



## INTERVIEW MELANI

# EIN INTENSIVERER AUSTAUSCH UND DIE ENTWICKLUNG VON KOMPETENZEN SIND ENTSCHEIDEND

**Welches sind die grössten Herausforderungen und Problembereiche in Bezug auf Cyber Security?**

Wir verzeichnen eine zunehmende Zahl an gezielten und professionell durchgeführten Angriffen. Einer Studie zufolge sind es vor allem KMU mit 10 bis 100 Beschäftigten, die immer stärker ins Visier dieser Attacken geraten. Die meisten Angreifer haben es auf finanzielle Ressourcen abgesehen, indem sie etwa Kreditkarten stehlen, Angriffe auf E-Banking-Kunden starten oder Wirtschaftsspionage betreiben (Spear Phishing). Angriffe auf kritische Infrastruktureinrichtungen, wie Kraftwerke, können schwere Folgen haben. Das Bewusstsein ist in vielen Unternehmen nicht hinreichend ausgeprägt, beispielsweise, wenn interne Informationen unverschlüsselt per E-Mail versendet werden. Wir stehen ständig in engem Kontakt mit über 100 Unternehmen, um diese dabei zu beraten, wie man sich heute am besten schützt. MELANI ist in der glücklichen Lage, ihren Kunden Informationen weiterleiten zu können, die öffentlich nicht zugänglich ist.

Eine weitere Herausforderung ist die Identifizierung und Festnahme der Eindringlinge (Hacker). Nicht alle Länder leisten der Schweiz Rechtshilfe. Darüber hinaus ist es extrem schwierig, den Aufenthaltsort dieser Eindringlinge festzustellen.

> Gezielte Angriffe nehmen zu und werden zunehmend professionell durchgeführt. Daher sind Unternehmen mehr denn je auf den gegenseitigen Wissensaustausch angewiesen. Das Cyberthema wird auf Unternehmensleitungsebene vielfach noch immer unterschätzt.
>
> Kernaussagen von Max Klaus, stellvertretender Leiter von MELANI, der Melde- und Analysestelle Informationssicherung in der Schweiz.

**Welches sind die Hauptmassnahmen, um die Anzahl und die Wirkung der Angriffe zu begrenzen?**

Der Austausch zwischen Unternehmen und der Regierung ist wichtig. Ohne diesen Austausch wird es extrem schwierig, sich isoliert gegen die neuartigsten Angriffe zu schützen. Wir organisieren zwei Mal jährlich Workshops mit den grössten Schweizer Unternehmen. Dies sind hauptsächlich Unternehmen aus den Sektoren Finanzen, Telekommunikation und Energie. In der Vergangenheit haben viele es nicht gewagt, offen über Angriffe zu sprechen. Heute sind die Unternehmer bereits offener und tauschen sich sogar mit direkten Wettbewerbern aus. Das ist eine, wie ich meine, sehr positive Entwicklung.

Eine weitere Massnahme ist die Schaffung von Know-how. Sehr häufig fehlt es in Unternehmen an den notwendigen technischen Fachleuten und/oder finanziellen Ressourcen.

Wir verwenden ein geschütztes Portal für den Austausch von Informationen mit unserem Kundenstamm. In unregelmässigen Abständen informieren wir KMUs und die Öffentlichkeit in einem Newsletter über Vorfälle, die unserer Einschätzung nach ein Risiko für die Mehrheit der Bevölkerung darstellen.

> Ohne Kooperationen wird es extrem schwierig, die eigene Organisation zu schützen.

**Viele Unternehmen investieren nicht in ihre IT, bevor sie tatsächlich einmal angegriffen werden. Was ist Ihre Erfahrung?**

Oft unterschätzt das Management das Thema Cyberrisiken, solange es keine Vorfälle gibt. Darüber hinaus sind Pläne, beispielsweise für das Kontinuitätsmanagement, häufig nur halbherzig formuliert. Findet bereits eine Attacke statt, ist keine Zeit zur Vorbereitung. Die Krisen- und Kommunikationspläne sowie die entsprechenden Prozesse müssen im Voraus implementiert werden.

**Können sich Unternehmen sicher fühlen, wenn sie die IT outsourcen?**

Outsourcing und Cloud Services können zu Problemen führen, weil die Daten einem externen Anbieter anvertraut werden. Man kann einfach nicht wissen, ob der Betreiber der Cloud verantwortlich mit den Daten umgeht, regelmässige Backups durchführt, keine Daten an Dritte weitergibt oder die Serverfarmen angemessen schützt. Outsourcing und Cloud Services sind nur für nicht vertrauliche Daten geeignet. Sensible Daten jedoch (Forschungsergebnisse, Konstruktionspläne etc.) sollten nach Möglichkeit im Kontrollbereich des Unternehmens bleiben.

**Wie steht die Schweiz im Vergleich mit anderen Ländern hinsichtlich der Cyber Security da?**

Im Wesentlichen ist die Schweiz denselben Bedrohungen ausgesetzt wie alle anderen Länder auch. Die Schweiz verfügt über eine nationale Cyberstrategie («Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken»), in der die Hauptrisiken erfasst sind, Massnahmen empfohlen werden und die Entwicklung von Kompetenzen berücksichtigt wird. Im Vergleich zu ähnlichen Strategien des Auslands hält die Schweizer Strategie spezifische Massnahmen und einen Plan zur Massnahmenumsetzung bereit. In den zehn Jahren ihres Bestehens hat die MELANI ein internationales Netzwerk zu ähnlichen Organisationen und Spezialisten auf der ganzen Welt sowie zu wichtigen Herstellerunternehmen (z.B. Microsoft, Google, Entwicklern von Antivirus-Software) aufgebaut. Diese Kontakte können der Schlüssel zum Erfolg sein, wenn es um die Abwehr zeitsensitiver Vorfälle geht.

Max Klaus

## INTERVIEW BASLER VERSICHERUNGEN

# ENTSCHEIDEND IST DAS PROBLEMBEWUSSTSEIN AUF MANAGEMENTEBENE

**Was bedeutet Informationssicherheit für die Basler Versicherungen?**
«Wir machen Sie sicherer» ist ein wesentlicher Bestandteil der Kultur und Zielsetzung der Basler Versicherungen. Selbstverständlich trifft dies auch auf die IT zu. Daher besteht seit Jahren in der Gruppe ein systematischer Ansatz für Informationsmanagement und IT-Sicherheit. Das Fortschreiten der Digitalisierung hat zu vermehrten Risiken im Zusammenhang mit dem Schutz sensibler Daten im Unternehmen sowie der Angreifbarkeit von IT-Systemen geführt.

**Welches sind die Haupttreiber dieser Risiken?**
Die Haupttreiber sind die zunehmende Vernetzung und die Interaktionen des Unternehmens mit Stakeholdern und Kunden über digitale Kanäle, die Verwendung mobiler Endgeräte mit Zugang zum IT-System und internen Daten des Unternehmens sowie die weltweite Professionalisierung der Cyberkriminalität. Die Basler Versicherungen passen die bestehenden Schutzmassnahmen kontinuierlich den neuen Bedrohungen und Risikoszenarien an. Das Thema Cyber Security hat, insbesondere dank starker Präsenz in den Medien, zu Fortschritten auf dem Gebiet des Informationssicherheitsmanagements beigetragen, namentlich in Bezug auf Prävention, Erkennung und Umgang mit entsprechenden Vorfällen.

> Das Thema Cyber Security hat, insbesondere dank starker Präsenz in den Medien, zu Fortschritten auf dem Gebiet des Informationssicherheitsmanagements beigetragen, namentlich in Bezug auf Prävention, Erkennung und Umgang mit entsprechenden Vorfällen.
>
> Kernaussagen von Olaf Romer,
> Head Corporate IT der Basler Versicherungen.

**Wie wichtig ist der menschliche Faktor?**
Ein integraler Bestandteil wirksamer Massnahmen ist die Schaffung eines Problembewusstseins unter den Mitarbeitenden und deren Schulung, denn vielen Angriffen sind Defizite in diesem Bereich geschuldet. Wir nutzen hierzu Aufklärungskampagnen mit Spielelementen (Gamification). Die etablierten Massnahmen haben sich bisher als wirksamer Schutz vor grösseren Vorfällen oder Datenverlusten erwiesen, aber hundert Prozent Sicherheit können nie garantiert werden. Der Umfang künftiger Investitionen in Cyber Security hängt stark vom Bewusstsein der Unternehmensleitung für die Angreifbarkeit des Unternehmens ab.

> Die Haupttreiber sind die zunehmende Vernetzung und die Interaktionen des Unternehmens mit Stakeholdern und Kunden über digitale Kanäle, die Verwendung mobiler Endgeräte mit Zugang zum IT-System und internen Daten des Unternehmens sowie die weltweite Professionalisierung der Cyberkriminalität.

**Olaf Romer**

# VERTEILUNG
## UMFRAGETEILNEHMER NACH SEKTOREN

**40,6%**
FINANZDIENSTLEISTUNGEN

**3,1%**
PHARMA

**4,7%**
INFRASTRUKTUR

**7,8%**
ENERGIE UND BODENSCHÄTZE

**4,7%**
KOMMUNIKATION/ UNTERHALTUNG

**9,4%**
ÖFFENTLICHE VERWALTUNG

**9,4%**
SONSTIGE DIENSTLEISTUNGEN

**3,1%**
GESUNDHEIT

**12,5%**
KONSUMGÜTER/ INDUSTRIE

**4,7%**
SONSTIGE

# UMFRAGE-METHODIK

KPMG hat diese Umfrage zu Cyber Security unter Schweizer Unternehmen im Jahr 2015 durchgeführt. Ziel der Umfrage ist es herauszufinden, wie Schweizer Unternehmen grundsätzlich den Herausforderungen der Cyber Security begegnen und ob sie Verfahren und Massnahmen eingeführt haben, die sie auch umsetzen. Die 64 Teilnehmer, 27 Grossunternehmen (> 5,000 FTE) und 37 kleine und mittlere Unternehmen (KMU), erhielten je 30 Fragen und haben diese individuell beantwortet. Ein weiterer Bestandteil dieser Studie sind persönliche Interviews mit Vertretern von fünf grossen Schweizer Unternehmen. Die Auswertung der Ergebnisse erfolgte durch ein Expertenteam von KPMG IT Advisory. Inhalt dieser Studie sind die Umfrage-Ergebnisse, die mit Erfahrungen aus der Beratungsarbeit von KPMG ergänzt wurden.

KPMG

# UNSER ANSATZ FÜR CYBER SECURITY

## KLARE ERKENNTNISSE

In der schnelllebigen digitalen Welt mit Bedrohungen und Chancen, die sich kontinuierlich verändern, braucht es Agilität, aber auch Sicherheiten. Unsere Mitarbeitenden sind Experten für Cyber Security, aber auch für Ihren Markt, so dass Sie von uns erstklassige Erkenntnisse, Ideen und erprobte Lösungen erhalten und mit diesen im Hintergrund überzeugt handeln können.

## SEITE AN SEITE

Wir arbeiten mit Ihnen als langfristige Partner zusammen, beraten Sie und hinterfragen Ihre Vorhaben, so dass Sie Ihre Entscheidungen mit Selbstvertrauen treffen können. Wir verstehen, dass auf diesem Gebiet Zweifel und Gefühle der Angreifbarkeit in die Entwicklung von Strategien hineinspielen. Daher arbeiten wir mit Ihnen Hand in Hand, um solche Bedenken in ein Gefühl von Sicherheit und sich eröffnenden Chancen zu verwandeln.

## IHRE UNTERNEHMERISCHE ZUKUNFT SICHERN

KPMG kann Ihnen helfen, Ihren Ansatz für Cyber Security umzubauen. Mit unserem Know-how, unserer Unterstützung und unseren kritischen Fragen verhelfen wir Ihnen trotz aller Komplexität zu verlässlicher Cyber Security. Auf Grundlage unserer Erfahrungen in vielen Sektoren und bei vielen Kunden haben wir einen klaren und wirksam gestaffelten Ansatz für mehr Cyber Security entwickelt.

## ORIENTIERUNG AN DEN GESCHÄFTSZIELEN

Gemeinsam mit Ihnen arbeiten wir daran, Ihr Unternehmen voranzubringen. Ein positives Management von Cyberrisiken hilft Ihnen nicht nur, Unsicherheiten in Ihrem Unternehmen unter Kontrolle zu bringen, sondern kann sich auch als echter strategischer Vorteil erweisen.

## GLOBAL, LOKAL

Im KPMG-Netzwerk arbeiten über 2.000 Fachleute weltweit als ein Team für mehr Cyber Security bei unseren Kunden. Das gibt uns die Möglichkeit, international kontinuierlich hohe Qualität zu erbringen. Die Mitgliedsfirmen von KPMG stehen Ihnen in fast jedem Land für lokale Bedürfnisse zur Seite, beginnend mit der Strategie für Informationssicherheit und Transformations-Programmen über technische Bewertungen, forensische Untersuchungen, Reaktionen auf Vorfälle, Schulungen bis hin zur Zertifizierung nach ISO 27000.

## KOOPERATIV

Wir errichten kooperative Foren und arbeiten mit diesen, um die besten Köpfe der Branche an einen Tisch zu bringen und gemeinsam Herausforderungen zu bewältigen. Das I-4-Forum von KPMG ist eine Plattform von über 50 der weltweit grössten Organisationen, in dem aufkommende Fragestelllungen und mögliche Antworten diskutiert werden.

# WIR SIND ...

## VERTRAUENSWÜRDIG

Wir verfügen über eine lange Liste von Zertifizierungen und Zulassungen, die uns befähigen, für die weltweit führenden Organisationen auf Mandatsbasis tätig zu sein.

## THEMENORIENTIERT

Wir bauen unsere Fähigkeiten stetig aus, um die steigende Nachfrage der Kunden nach einem verlässlichen Schutz ihrer Informationen und nach Business Resilience Services zu erfüllen.


W3nn du d45
l353n k4nn57
b3wlrb dich
b31 KPM6!
kpmg.ch/cyberjobs

# Clarity on

## Online-Publikationen

Die Reihe «Clarity on» von KPMG bietet eine breite Palette an Studien, Analysen und Erkenntnissen. Mehr Informationen finden Sie auf kpmg.ch/clarity-on.

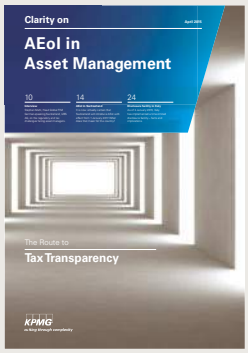
Die neuesten Ausgaben


Clarity on **Investment in Switzerland**


Clarity on **Performance of Swiss Private Banks**


Clarity on **Digital Transformation**


Clarity on **Swiss Taxes**




Clarity on **AEoI in Asset Management**


Clarity on **Mergers & Acquisitions**


Clarity on **Life Insurance matters**


Clarity on **Healthcare**


Clarity on **Commodities Trading**


Clarity on **The Future of Swiss Private Banking**

**Clarity on**
kpmg.ch/clarity-on

## Knowledge App von KPMG

Holen Sie sich direkten Zugang zum Wissen der Spezialisten von KPMG mit der «Knowledge App» für iPad – jetzt sogar noch kompakter und spezifisch auf Ihre Bedürfnisse abstimmbar.

Available on the App Store

**Knowledge App von KPMG**
kpmg.ch/knowledge

IMPRESSUM UND KONTAKT

Für weitere Informationen über
**Clarity on Cyber Security**
wenden Sie sich bitte an:

**Matthias Bossardt**
Partner, Cyber Security
+41 58 249 36 98
mbossardt@kpmg.com

**Jean-Paul Ballerini**
Senior Manager, Cyber Security
+41 58 249 55 64
jballerini@kpmg.com

**Gerben Schreurs**
Partner, Cyber Security
+41 58 249 48 29
gschreurs1@kpmg.com

**Roman Haltinner**
Senior Manager, Cyber Security
+41 58 249 42 56
rhaltinner@kpmg.com

**Anne van Heerden**
Partner, Head of Advisory
+41 58 249 28 61
annevanheerden@kpmg.com

**Ulrich Amberg**
Partner, Head of IT Advisory
+41 58 249 62 62
uamberg@kpmg.com

**Herausgeber**
KPMG AG
Badenerstrasse 172
Postfach
8036 Zürich
+41 58 249 31 31
+41 58 249 44 06 (Fax)
kpmgpublications@kpmg.ch

**Redaktionsteam KPMG**
Matthias Bossardt
Gerben Schreurs
Jean-Paul Ballerini
Roman Haltinner
Rikard Sandström
Konrad Schwenke

**Konzept und Design**
KPMG, Stephan Erdmann
KPMG, Irene Hug
Konkret, Andi Portmann

**Druck**
GfK PrintCenter, Hergiswil

**Bilder**
Shutterstock


**Clarity on Cyber Security**
kpmg.ch/cyber