techconsult
The IT Market Analysts

1. **Bericht zur Studie „Security-Bilanz Deutschland“**

   Der Status Quo der IT-Sicherheit im deutschen Mittelstand

   -- Kurzbericht --

SecurityBilanz

EINE STUDIE ZUR
IT- UND INFORMATIONSSICHERHEIT
KLEINER UND MITTELSTÄNDISCHER UNTERNEHMEN
IN DEUTSCHLAND

techconsult The IT Market Analysts | Heise | SecurityConsulter

Studienbeirat:

heise Security | TeleTrusT Pioneers in IT security. | wecon.it-consulting »we.secure-your.it« | Bundesamt für Sicherheit in der Informationstechnik | BITKOM

Partner:

baramundi software AG | IBM | mesh | Microsoft

NCP SECURE COMMUNICATIONS | SOPHOS Security made simple. | T | brainloop | TREND MICRO

Inhalt

Copyright

Disclaimer

Der vorliegende Bericht ist eine gekürzte Fassung des Studienberichts zur Studie *Security Bilanz Deutschland*. Den Studienbericht mit detaillierten Untersuchungen der Maßnahmen und Lösungen auf allen relevanten Ebenen von IT- und Informationssicherheit finden Sie im Mitgliederbereich nach einer kostenfreien Registrierung auf der Projektseite **https://www.security-bilanz.de**.

Außerdem steht dort für Sie der auf der Studie aufbauende **Sicherheitscheck *Heise Security Consulter*** bereit, mit dem Sie sich mit den Studienergebnissen vergleichen können – *machen Sie den Sicherheitscheck!*

Vorwort

Nicht erst seit den jüngsten Skandalen rund um die Nachrichtendienste dieser Welt befassen sich Unternehmen mit der Frage nach IT- und Informationssicherheit und den entsprechenden Schutzmaßnahmen. Doch wie sieht der Status quo in deutschen Unternehmen hinsichtlich IT- und Informationssicherheit aus? Wie sicher fühlt sich der Mittelstand? Wie schätzen Unternehmen ihre Maßnahmen selbst ein? Wo liegen Probleme, vor allem auf welcher Ebene?

Ziel des Projektes ist, die Themen IT-Sicherheit und Informationssicherheit im Mittelstand umfassend zu betrachten. Zentrales Anliegen war dabei, mittelständische Unternehmen dabei zu unterstützen, die eigene IT- und Informationssicherheit zu verbessern. Ein Ausgangspunkt dafür ist die vorliegende Studie. Sie liefert ein umfassendes Gesamtbild, wie der deutsche Mittelstand hinsichtlich IT- und Informationssicherheit aufgestellt ist.

Eine weitere Anforderung neben dieser Statusaufnahme war von vornherein der Anspruch auf Nachhaltigkeit. Um die Entwicklung von IT- und Informationssicherheit im Mittelstand zu begleiten und ihre Transparenz zu erhöhen, ist vorgesehen, die Studie jährlich zu wiederholen. techconsult kann auf umfangreiche Erfahrungen aus zahlreichen Individual- und Standarduntersuchungen im Mittelstand zurückgreifen. Diese richten sich seit jeher am Anspruch der Nähe zum Anwenderunternehmen aus und verfügen über eine einzigartige Breite und Tiefe.

Die Studie *Security Bilanz Deutschland* ist ein Gemeinschaftsprojekt der techconsult GmbH und des Heise Zeitschriften Verlags. Für die Mitwirkung konnten Günter Ennen (BSI), Joerg Heidrich (Heise Verlag), Jürgen Schmidt (heise security), Dr. Christoph Wegener (wecon.it-consulting), Dr. Holger Mühlbauer (TeleTrust) und Marc Fliehe (BITKOM) als Fachexperten für den Studienbeirat gewonnen werden.

Im Partnerbeirat haben Armin Leinfelder (baramundi), Claudia Gharavi (mesh), Michael Kranawetter (Microsoft Deutschland),

Jürgen Hönig (NCP), Jörg Schindler (Sophos) und Ursel Graubmann (Telekom Deutschland) das Projekt als Experten von Anbieterseite unterstützt und wertvolle Anregungen aus ihren Praxiserfahrungen eingebracht. Darüber hinaus wird die Studie unterstützt von Brainloop und Trend Micro.

Sie alle haben entscheidend mit zum Gelingen dieses Projektes beigetragen – ein herzlicher Dank an dieser Stelle für Ihr Engagement!

Die Studienergebnisse bilden darüber hinaus die Basis für einen Online-Self-Check, den *Heise Security Consulter*. Wir möchten Sie dazu einladen, diesen Self-Check durchzuführen und so eine Standortbestimmung hinsichtlich IT-Sicherheit in Ihrem Unternehmen vorzunehmen. Sie erhalten sofort eine Auswertung inklusive eines Vergleichs mit den Ergebnissen der hier vorgestellten Studie, das heißt mit Unternehmen Ihrer Branche und Größenklasse, und können schnell erkennen, wo eine Änderung Ihrer Situation nötig wäre.

Hannover und Kassel, April 2014

techconsult GmbH

Zur Einleitung: Idee und Studienkonzept

Grundsätzlich geht man davon aus, dass der Mittelstand nicht in der Lage ist, die notwendigen Maßnahmen zu ergreifen, um den sich ständig ändernden und ganzheitlich zu betrachtenden Anforderungen an IT-Sicherheit, Datenschutz und Informationssicherheit gerecht werden zu können. Ist dies wirklich so? Wie gut aufgestellt fühlen sich mittelständische Unternehmen in der technischen aber auch rechtlichen und organisatorischen Umsetzung von IT- und Informationssicherheit? Das Ziel der hier vorgestellten Studie ist es, den Status quo von IT- und Informationssicherheit im deutschen Mittelstand zu erheben.

Ganzheitliche Betrachtung

Das Studienkonzept ist dabei darauf ausgerichtet, eine möglichst umfassende Betrachtung des Themas IT-Sicherheit in mittelständischen Unternehmen vorzunehmen. Dabei werden verschiedene Ebenen unterschieden: die technische, organisatorische, rechtliche und strategische Ebene. Auf jeder dieser Ebenen werden Klassen von Lösungen oder Maßnahmen angesprochen, um so auf der einen Seite ein umfassendes Bild zu ermitteln, auf der anderen Seite aber auch eine sinnvolle Detailtiefe rund um die Themen IT- und Informationssicherheit zu ermöglichen.

Selbsteinschätzung der Unternehmen

Die Grundlage dafür bilden die Selbsteinschätzungen der Unternehmen. Diese Selbsteinschätzungen wurden nach dem von techconsult seit Jahren erfolgreich eingesetzten zweidimensionalen Relevanz-Umsetzungs-Schema erhoben: Welche Maßnahmen und Lösungen sind für die Unternehmen wichtig und wie zufrieden sind die Unternehmen mit deren Umsetzung?

Zusätzlich wurden IT- und Informationssicherheit aus unterschiedlichen Perspektiven betrachtet: Zum einen wurde der Fokus darauf gesetzt, welche Maßnahmen Unternehmen selbst treffen können, um IT- und Informationssicherheit sicher zu stellen. Dabei wurden unterschiedlichste Kommunikations- und Austauschbeziehungen mit Partnern, Kunden, Lieferanten, Behörden usw. berücksichtigt, in denen Unternehmen stehen. Zum an-

deren wurden aber auch die Bedrohungen in den Blick genommen, welche von innen und außen auf Unternehmen einwirken und ermittelt, wie gut die Absicherung gegen diese Bedrohungen eingeschätzt wird.

Der Fragebogen umfasste ca. 40 Fragen, die in detaillierter aber verständlicher Art und Weise den Sicherheitsstatus eines mittelständischen Unternehmens behandeln und trotz Komplexität von einem normalen Mitarbeiter beantwortet werden konnten. Unter anderem behandelte der Fragebogen folgende Themen:

- Relevanz, Anforderungen und Umsetzung von IT- und Informationssicherheit in verschiedenen Unternehmensbereichen
- Maßnahmen, Regelungen und Strategien zur IT- und Informationssicherheit, untergliedert in vier Ebenen:
  - Technische Ebene
  - Organisatorische Ebene
  - Rechtliche Ebene
  - Strategische Ebene
- Bedrohungslage, Ausfälle und Handlungsbedarfe im letzten Jahr

Gesamtergebnis im Überblick

INDIZES IM BRANCHENVERGLEICH

Zur Zusammenfassung der detaillierten Betrachtung auf technischer, organisatorischer, rechtlicher und strategischer Ebene wurde ein Index gebildet, der als oberster Vergleichswert dient: der *Sicherheitsindex*. Dieser Indexwert stellt den Grad der Relevanz und Umsetzung einer großen Anzahl von theoretisch möglichen Lösungen und Maßnahmen auf den verschiedenen Ebenen dar, die in Unternehmen realisiert werden, um IT- und Informationssicherheit zu gewährleisten (siehe auch S. 17, Methodik der Indexbildung).

Sicherheitsindex

Abbildung 1 zeigt die ermittelten Werte für die befragten mittelständischen Unternehmen insgesamt sowie für die untersuchten Branchen: Der Indexwert für das Sicherheitspotenzial erreicht im Gesamtdurchschnitt 57 von 100 Punkten. Dieses Niveau zeigt deutlich, dass der Mittelstand noch weit von einer vollständigen Beherrschung der relevanten Sicherheitsaspekte entfernt ist.

Weiterhin offenbart sich, dass es deutliche Unterschiede zwischen den Branchen gibt. So führt die Industrie mit 60 Indexpunkten knapp vor den Banken und Versicherungen mit 59 Punkten das Feld an. Die Dienstleister liegen mit 57 Punkten genau im Durchschnitt. Öffentliche Verwaltungen und Non-Profits liegen mit 54 Punkten drei Zähler unter dem Schnitt, das Schlusslicht bildet der Handel mit nur 52 Punkten.

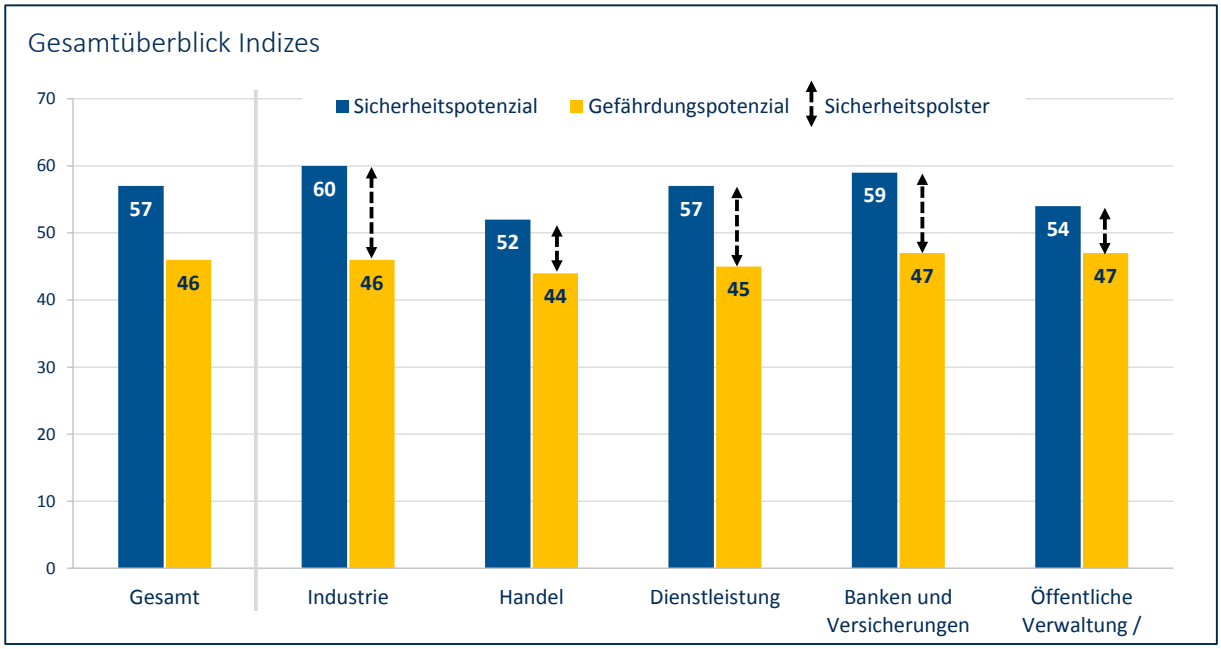

Abbildung 1: Indizes im Branchenvergleich

Das theoretische Maximum der Indexwerte beträgt jeweils 100 Punkte. Das praktikable und für den Geschäftsbetrieb akzeptable Maß liegt niedriger, sollte aber nicht weit von den als „Best Practice" einzustufenden Werten von rund 80 Punkten liegen (s.u.). „Hundertprozentige IT-Sicherheit" ist bekanntermaßen auch nicht zu erreichen. Neben den Anforderungen hinsichtlich IT- und Informationssicherheit muss schließlich auch sichergestellt sein, dass das Unternehmen seiner eigentlichen Tätigkeit weiterhin nachgehen kann, also z.B. Produktion und Verkauf weitestgehend ungehindert fortgesetzt werden können.

Gefährdungsindex

Weiterhin ist ein Index für das *Gefährdungspotenzial* gebildet worden, der die Bedrohungslage und den Schutz vor diesen Bedrohungen abbildet. „Bedrohung + Schwachstelle = Gefährdung"[1] – so einfach und doch treffend fällt die Definition des Bundesamt für Sicherheit in der Informationstechnik (BSI) aus. Der Gefährdungsindex bildet genau diese beiden Größen ab: Zum einen die von Unternehmen wahrgenommene Bedrohung,

1 Bundesamt für Sicherheit in der Informationstechnik (BSI), „Begriffserläuterung und Einführung", https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Themen/Sicherheitsvorfaelle/Begriffserlaeuterungen/Begriffserlaeuterungen_node.html.

zum anderen das Vorhandensein von potenziellen Schwachstellen, die sich in Unzufriedenheit oder Zufriedenheit mit der Umsetzung des Schutzes manifestieren. Ein hoher Gefährdungsindex bedeutet somit, dass eine hohe Bedrohung wahrgenommen wird, gegen die man sich nicht gut geschützt fühlt. Ein niedriger Wert hingegen bedeutet, dass die Bedrohung geringer eingeschätzt wird und/oder auch der Schutz vor Bedrohungen besser umgesetzt ist.

Großer Punkte-Vorsprung der sicheren Unternehmen

Dass die ermittelten Werte nur als befriedigend oder ausreichend zu interpretieren sind, zeigt auch die große Spanne in den Ergebnissen. Abbildung 2 zeigt, dass die besten 25 % der Unternehmen Durchschnittwerte jenseits der 78-Punkte-Marke erreichen. Unternehmen, die gut bis sehr gut hinsichtlich IT- und Informationssicherheit aufgestellt sind, erreichen also mehr als 20 Punkte höhere Indexwerte. Die 25 % schlechtesten Unternehmen erreichen nur Werte von 38 Punkten oder weniger.

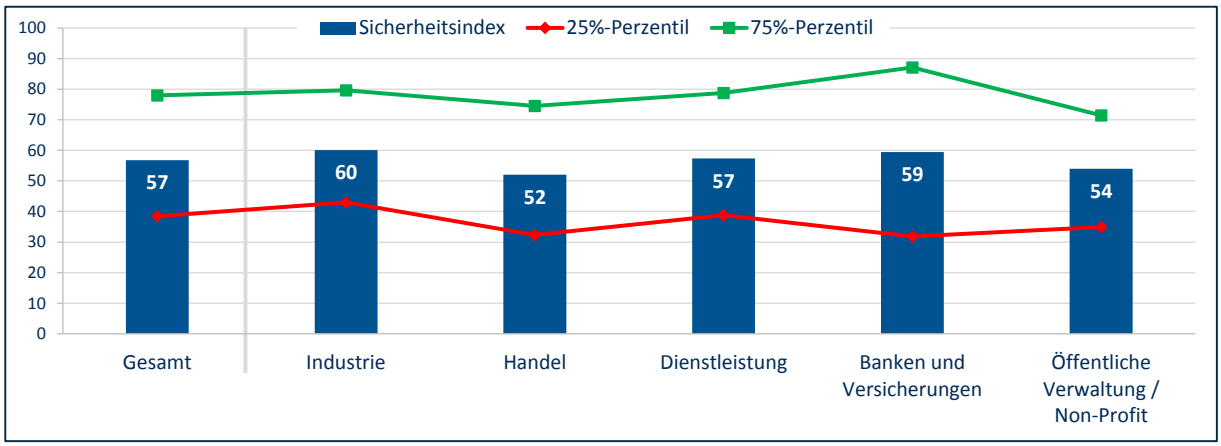

Abbildung 2: Spanne der Ergebnisse beim Sicherheitsindex

Mittelstand sieht sich keiner dramatischen Bedrohung ausgesetzt

Die Gefährdung, der sich die Unternehmen ausgesetzt sehen, führt zu einem Indexwert von 46 Punkten. Die einzelnen Branchen unterscheiden sich hier nur marginal, es herrscht weitgehend Einigkeit. Im Handel liegt das wahrgenommene Gefährdungspotenzial leicht niedriger bei 44 Punkten, bei Banken und Versicherungen sowie Öffentliche Verwaltungen und Non Profits liegt der Indexwert mit 47 Punkten leicht höher. Der Index für das Gefährdungspotenzial ist als vergleichsweise durchschnittlich ausgeprägt zu interpretieren. Werte von unter 50 Punkten legen

den Schluss nah, dass sich die Befragten keiner dramatischen Bedrohung ausgesetzt sehen und ihre Schutzmaßnahmen subjektiv als ausreichend empfinden. Auch ist die Spanne der Einschätzungen deutlich geringer, als dies beim Sicherheitsindex der Fall ist (vgl. Abbildung 3). Diese Einschätzung einer relativ geringen Gefährdung ist vor dem Hintergrund der nur marginal höheren Einschätzung der eigenen Sicherheitsmaßnahmen trügerisch.

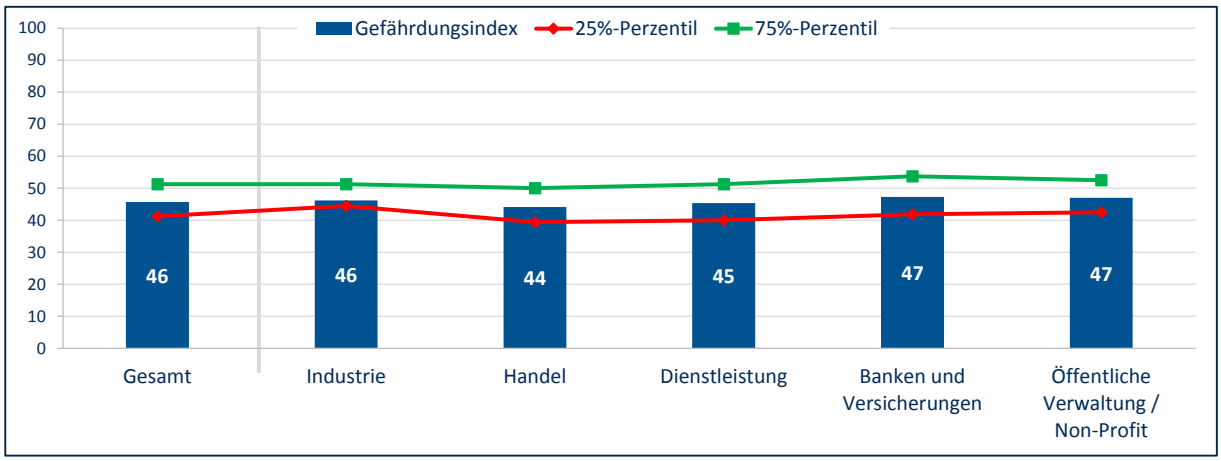

Abbildung 3: Spanne der Ergebnisse beim Gefährdungsindex

Trügerische Sicherheit: Sicherheitsvorsprung nur gering

Der Mittelstand, inkl. der öffentlichen Verwaltungen und Non-Profit Organisationen, zeigt sich somit erst einmal von der unsicheren Seite: Zur maximal möglichen Ausschöpfung ist es noch ein weiter Weg. Das Sicherheitspolster von 11 Punkten des gemessenen Sicherheitsempfindens (57 Punkte) gegenüber dem Gefährdungsempfinden (46 Punkte) stellt praktisch keinen Vorsprung dar. Wäre die Gefährdungswahrnehmung genauso hoch wie das Sicherheitsempfinden, so würde dies bereits eine sehr kritische Sicherheitslage darstellen, da keinerlei Spielräume für unkalkulierbare/nicht bekannte Risiken bestünden. Vor diesem Hintergrund sollte der wahrgenommene Gefährdungsindex maximal halb so hoch sein, wie der Wert des wahrgenommenen Sicherheitsempfindens. Aktuell haben mittelständische Unternehmen und Organisationen also nicht nur deutlichen Nachholbedarf in Richtung einer bestmöglichen Aufstellung in Sachen Datenschutz und Informationssicherheit, sondern sind zu dem auch nur bedingt geeignet, dem selbst wahrgenommenen Gefährdungspotential standzuhalten.

Sicherheitsindex im Detail

Der von den Unternehmen realisierte Sicherheitsindex ergibt sich aus vielen einzelnen Lösungen, Maßnahmen und Regelungen, die zur Sicherstellung von IT- und Informationssicherheit umgesetzt werden. Diese Lösungen, Maßnahmen und Regelungen lassen sich nach den verschiedenen Ebenen unterscheiden, die sie adressieren: Die technische, organisatorische, rechtliche und strategische Ebene.

Diese Ebenen können als gleichberechtigt angesehen werden. Jede dieser Ebenen muss im Unternehmen adressiert sein. Wenn es keine Umsetzung auf organisatorischer Ebene gibt, kann dieses Defizit nicht durch Lösungen auf technischer Ebene kompensiert werden. Die Strategie hält darüber hinaus alles zusammen und verankert IT- und Informationssicherheit im Unternehmen.

Technisch und rechtlich Top, organisatorisch und strategisch Flop

Beim Vergleich der Indexwerte der verschiedenen Ebenen zeigt sich deutlich, dass die Performance auf technischer und rechtlicher Ebene deutlich besser ausfällt, als auf organisatorischer oder strategischer Ebene (vgl. Abbildung 4). In allen untersuchten Branchen gibt es Defizite auf der strategischen Ebene. Bei fast allen bestehen ebenso Defizite auf organisatorischer Ebene, nur öffentliche Verwaltungen/Non-Profit-Unternehmen schneiden hier besser ab. Am relativ besten ist insgesamt die technische Ebene umgesetzt, allein der Handel erzielt auf rechtlicher Ebene höhere Indexwerte.

Die Industrie zeigt mit nah beieinander liegenden Ebenen-Indizes, dass sie am systematischsten an die Umsetzung von IT- und Informationssicherheit heran geht, trotzdem liegen auch hier die Indexwerte für die organisatorische und strategische Ebene niedriger als die der technischen und rechtlichen Ebene.

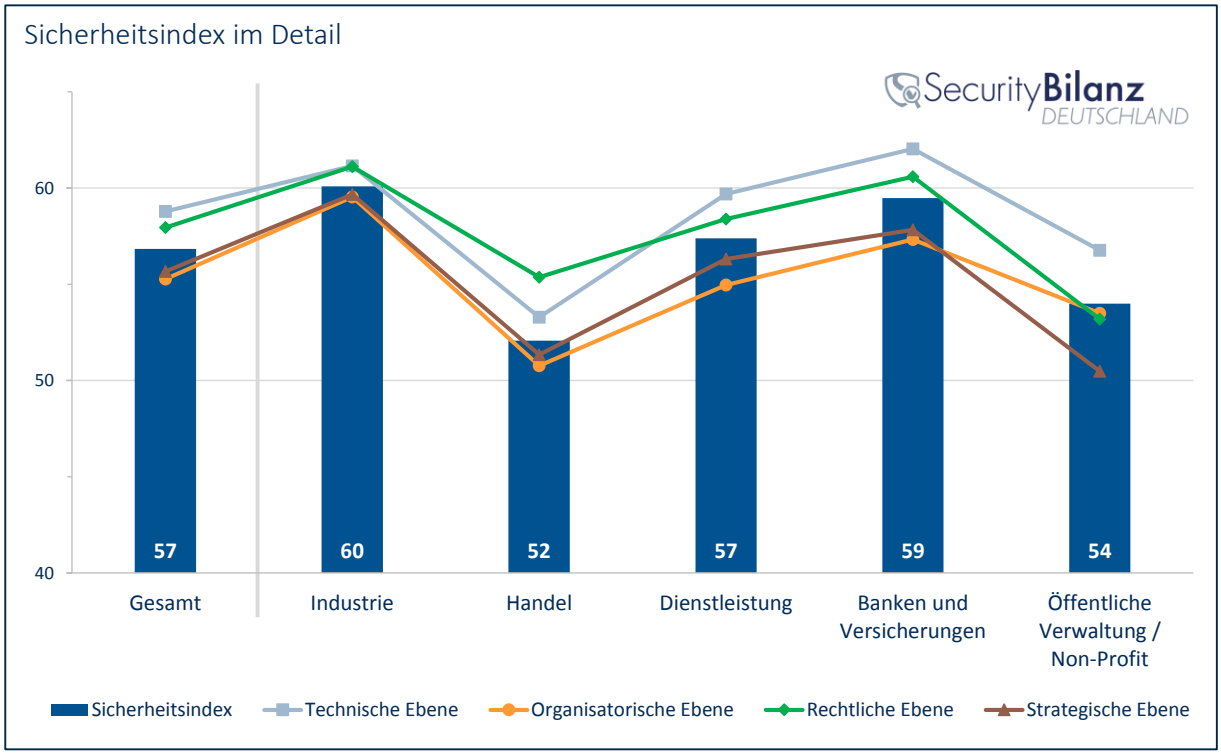

Abbildung 4: Sicherheitsindex im Detail

Eine detaillierte Untersuchung der Maßnahmen und Lösungen, die auf der technischen, organisatorischen und strategischen Ebene umgesetzt werden sowie vollständige Darstellungen der ermittelten Indexwerte für technische Maßnahmen und Lösungen sind im Detailbericht zu finden, der nach einer kostenfreien Registrierung auf der Projektseite https://www.security-bilanz.de zum Download bereitsteht.

Gefährdungsindex: Bedrohungslage und gefühlter Schutz

Der Gefährdungsindex veranschaulicht das Verhältnis von wahrgenommener Bedrohung und der Einschätzung des umgesetzten Schutzniveaus. Der durchschnittliche Gefährdungsindex aller befragten Unternehmen beträgt 46 Punkte.

Die abgefragten Szenarien wurden zwar insgesamt als Bedrohungen erkannt, jedoch wird das resultierende Gefährdungspotential als überschaubar und handhabbar angesehen. Der Mittelstand fühlt sich somit vor diesen gängigen Bedrohungslagen angemessen geschützt. Besonders bemerkenswert ist der Umstand, dass dabei keine der gängigen Bedrohungslagen herausticht. Die Unternehmen sehen sich aktuell gut aufgestellt und haben für verschiedene Bedrohungen angemessene Schutzvorkehrungen getroffen (vgl. Abbildung 5).

Gefährdungen	Gefährdungssindex
Datenverlust durch Unachtsamkeit und Fehlverhalten der Mitarbeiter (Geräteverlust, versehentliche Löschung etc.)	47
Interne Angriffe (z.B. Datendiebstahl, Sabotage)	46
Phishing und Social Engineering	46
Befall unserer Systeme durch Schadsoftware wie Viren und Würmer	46
Systemausfälle und Datenverlust durch Systemausfälle (Hardware-Defekte, Software-Fehler etc.)	46
Denial-of-Service-Attacken (Angriffe mit dem Ziel, die Verfügbarkeit unserer Systeme zu verringern)	46
Aushebelung der Zugangsbeschränkungen durch eigene Mitarbeiter	45
Unbefugter Zugang zu unseren Systemen und Daten (Trojaner, Hackerangriffe, Spyware)	45

https://www.security-bilanz.de © 2014 techconsult GmbH

Abbildung 5: Gefährdungen im Mittelstand

In der Betrachtung der wahrgenommenen Gefährdung auf Branchenebene sind zwei erhöhte Werte beim Gefährdungsindex auffällig. Banken und Versicherungen sehen sich bei internen Angriffen mit 53 Punkten beim Gefährdungsindex einer um 7 Punkten höheren Gefährdung ausgesetzt als dies im Mittelstandsdurchschnitt der Fall ist. Ebenso sehen sich öffentliche Verwaltungen und Non-Profits besonders durch Datenverlust durch Unachtsamkeit und Fehlverhalten der Mitarbeiter (Geräteverlust, versehentliche Löschung etc.) gefährdet, was in 53 Punkten beim Gefährdungsindex resultiert.

Vermeintlich positiv fällt der Gefährdungsindex für Systemausfälle und Datenverlust durch Systemausfälle (Hardware-Defekte, Software-Fehler etc.) im Handel aus. Nach der Einschätzung der befragten Handelsunternehmen ist die Bedrohung hier relativ gesehen niedriger, und die Schutzmaßnahmen sind besser umgesetzt.

Insgesamt zeigt das Niveau beim Gefährdungsindex jedoch im Vergleich mit dem Sicherheitsindex, dass sich aus der Selbsteinschätzung der Mittelständler im Durchschnitt nur einen geringer Sicherheitsvorsprung als Puffer ergibt (vgl. auch oben, Abbildung 1). Daraus ergibt sich, dass die Sicherheit, in der sich der Mittelstand wähnt, schnell in einen akuten Ernstfall umschlagen kann, z.B. weil sich die Bedrohungslage durch Bekanntwerden von Schwachstellen erhöht.

Gerade auch die große Spanne in der Selbstbewertung der eigenen Sicherheitslage (vgl. oben, Abbildung 2) zeigt, dass in vielen Fällen auch konkreter Handlungsbedarf besteht. Im Durchschnitt liegt ein Viertel der mittelständischen Unternehmen unter einem Sicherheitsindex-Wert von 40 Punkten. Bei der Einschätzung der Gefährdung liegen die Indexwerte jedoch deutlich näher beieinander. Hier liegt die Hälfte der befragten Unternehmen in einem Bereich zwischen 41 und 51 Punkten für den Gefährdungsindex. Dies legt den Schluss nahe, dass auch bei einem Viertel der Unternehmen dringender Handlungsbedarf besteht, weil ihr Sicherheitsniveau niedriger als das Gefährdungsniveau liegt, dem sie sich ausgesetzt sehen.

Studienrahmen

Die Befragung wurde im Januar und Februar 2014 durchgeführt. Mittels Computer Aided Web Interview (CAWI) wurden insgesamt 503 Personen befragt.

Die Branchenverteilung (vgl. Abbildung 6) zeigt einen Schwerpunkt im Dienstleistungssegment, dem insgesamt rund 44 % der befragten Unternehmen angehören.

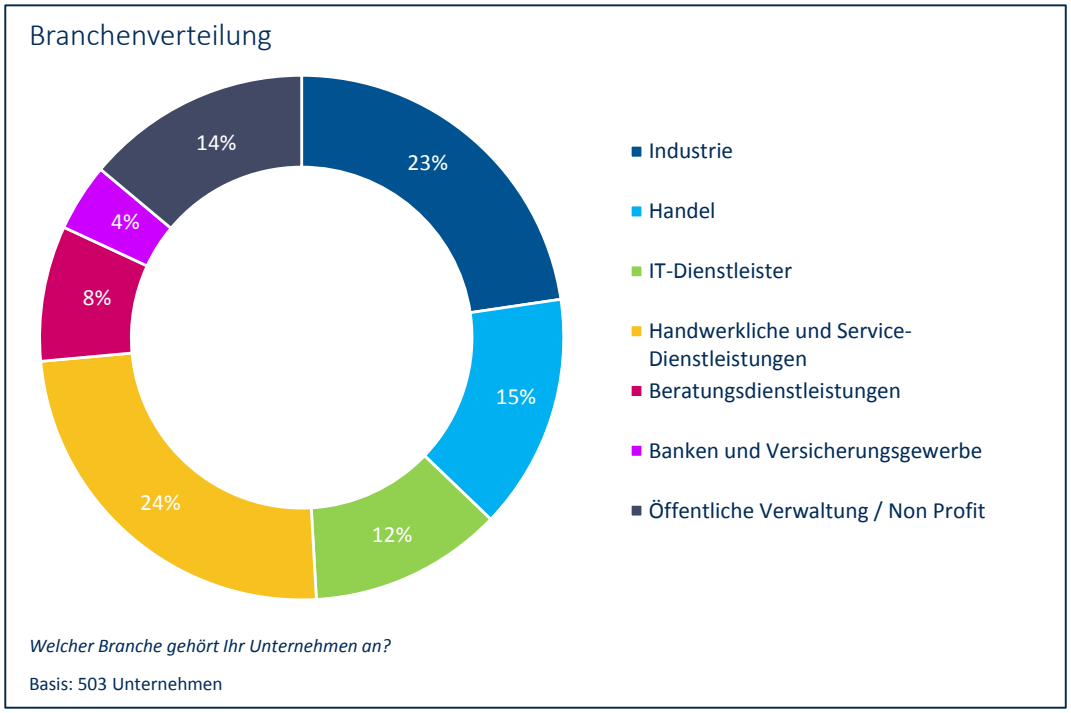

Abbildung 6: Branchenverteilung

Die IT-Dienstleister sind dabei mit 12 % Anteil bewusst etwas überrepräsentiert, um diese Gruppe in einer der diesem Bericht folgenden Detailauswertungen genauer untersuchen zu können. Schließlich sind sie gerade für kleinere Mittelständler die ersten Ansprechpartner, wenn es um die Umsetzung von Sicherheitskonzepten geht.

Nach Größenklassen betrachtet macht die Gruppe der mittelständischen Unternehmen mit 20 bis 199 Mitarbeitern mit 41 % den größten Anteil der Befragten aus, gefolgt von mittelgroßen Mittelständlern mit 200 bis 499 Mitarbeitern, die einem Drittel

vertreten sind und dem großen Mittelstand mit 500 bis 1.999 Unternehmen, denen ein Viertel der Befragten angehört (vgl. Abbildung 7).

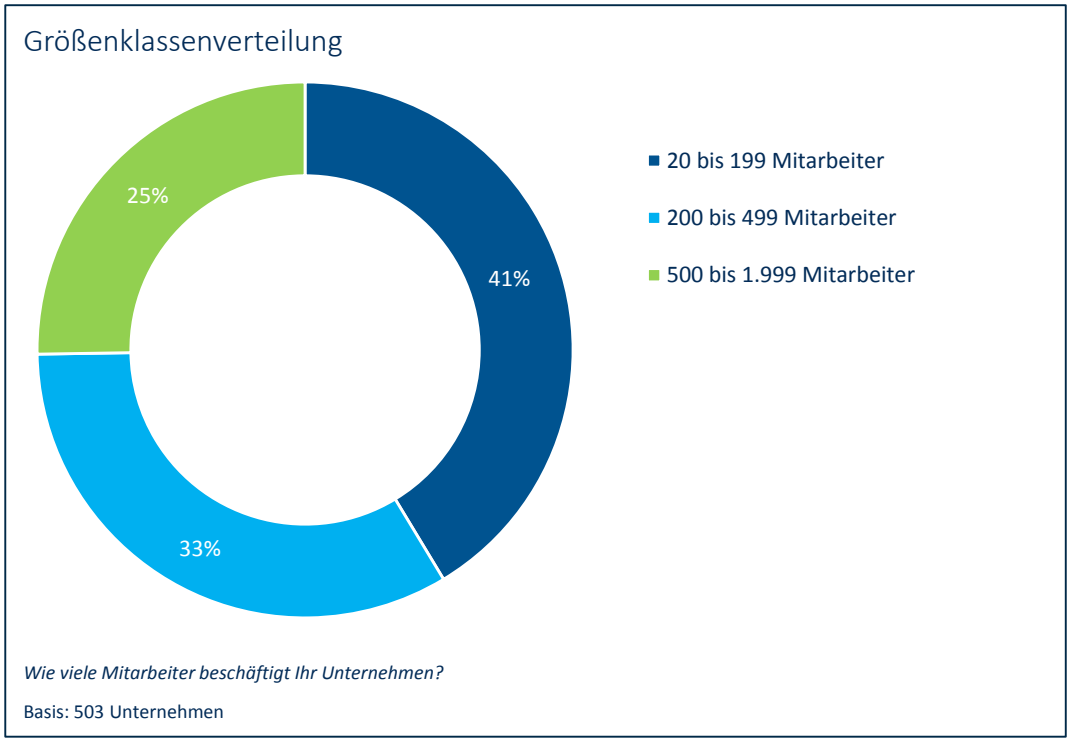

Abbildung 7: Verteilung der Größenklassen der Unternehmen

Die in der Studie befragten Personen sollten zu IT- und Informationssicherheit im eigenen Unternehmen Aussagen treffen können. Daher findet sich ein hoher Anteil von IT-Leitern und IT-Mitarbeitern (38 %) unter den Befragten. Fast ebenso viele der befragten Personen haben leitende Funktionen inne oder gehören der Geschäftsführung bzw. dem Vorstand an (37 %).

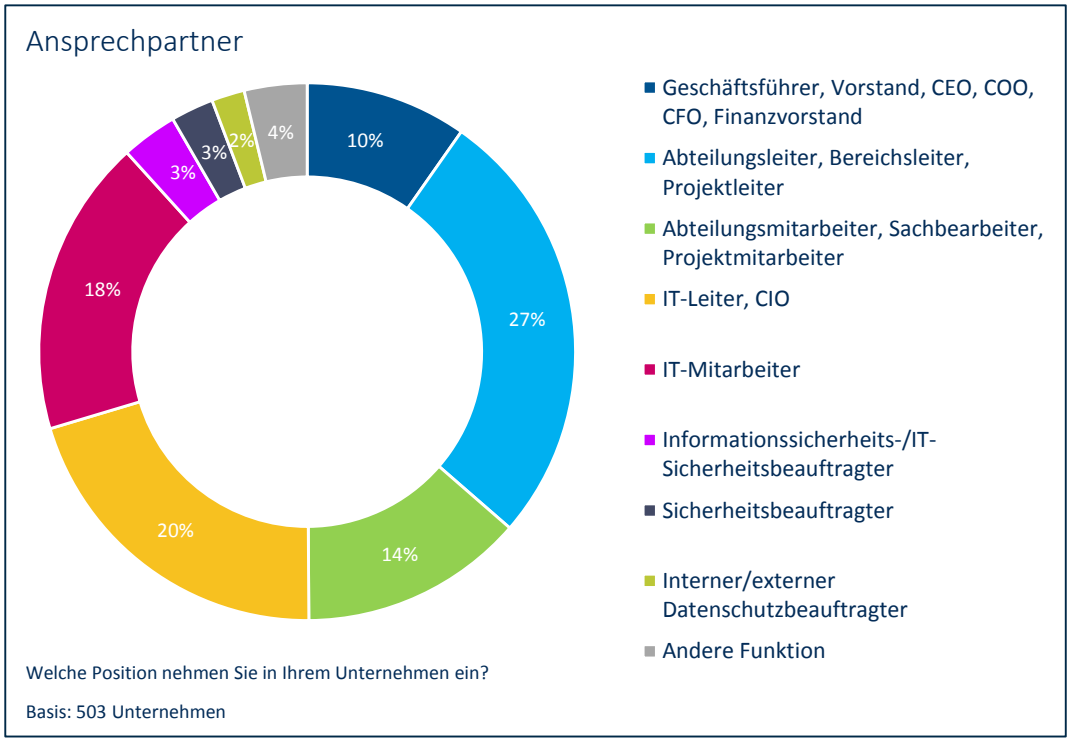

Abbildung 8: Ansprechpartner der Studie

Methodik der Indexbildung

Ein Ziel der Studie war es, auf oberster Ebene Indizes zu erstellen, die als Maßzahlen für Vergleiche dienen können. Die Idee dahinter ist mit einem Benchmark zu vergleichen. Diese Indizes sind zum einen der Sicherheitsindex, der die Umsetzung von IT- und Informationssicherheit im Unternehmen fokussiert, zum anderen der Gefährdungsindex, der die Bedrohungen und die Absicherung gegen diese Bedrohungen betrachtet.

Diese Methodik hat sich seit Jahren in unterschiedlichen Indexprojekten (z.B. Business Performance Index) bewährt und wurde kontinuierlich weiterentwickelt. Die Indexwerte ergeben sich dabei jeweils aus der Relevanz und Umsetzung von Maßnahmen und Lösungen bzw. der wahrgenommenen Bedrohung durch und des Schutzes vor bestimmten Gefahren. Diese basieren auf der Selbsteinschätzung der befragten Unternehmen und wurden jeweils mittels einer 6er-Skala (1=sehr hohe Relevanz bzw. sehr zufrieden mit der Umsetzung bis 6=überhaupt nicht relevant bzw. überhaupt nicht zufrieden mit der Umsetzung) erhoben. Für die Indexbildung werden diese Angaben auf Werte zwischen 0 und 100 transformiert und aggregiert. Die Aggregation erfolgt beim Sicherheitsindex zum einen auf den Teilebenen (technische, organisatorische, rechtliche und strategische Ebene) und zum anderen auch zusammenfassend als Gesamtwert (vgl. Abbildung 9).

Die „Umsetzung“ und die „Absicherung“ dienen als eigentliche Dimensionen zur Indexbildung, denn letztlich entscheiden getroffene Maßnahmen über die Sicherheit im Unternehmen. Jedes Unternehmen ist aber anders, hat andere Schwerpunkte und Prozesse zu berücksichtigen und ganz sicher haben die jeweiligen Akteure in den Unternehmen auch unterschiedliche Wahrnehmungen. Daher ist es nur folgerichtig, dass es keinen einheitlichen Maßnahmenkatalog zur Absicherung geben kann. Wir berücksichtigen diese Unterschiedlichkeit mit der Einführung einer Gewichtung. Für den Sicherheitsindex heißt diese Gewichtung

„Relevanz“, für den Gefährdungsindex „Bedrohung“. Der Umsetzung einer Maßnahme innerhalb eines Bereiches (technisch, strategisch, rechtlich, etc.) wird also die Relevanz gegenübergestellt, die diese Maßnahme nach Einschätzung der Befragten für das Unternehmen hat. So fällt eine hohe Umsetzung letztlich weniger ins Gewicht, wenn die Relevanz für einen Bereich unerheblich ist. Andersherum wird es entsprechend kritischer, wenn einer sehr hohen Relevanz nur eine geringe Umsetzung gegenüber steht. Die abgefragte Relevanz fungiert demnach als Gewichtungsfaktor. Analog dazu steht die „Bedrohung“ als Gewichtungsfaktor für die Absicherung. Wenn in einem bestimmten Bereich eine erhöhte Bedrohungslage festgestellt wird, ist der Absicherung eine höheres „Gewicht“ beizumessen, als in einem nicht akut bedrohtem Bereich.

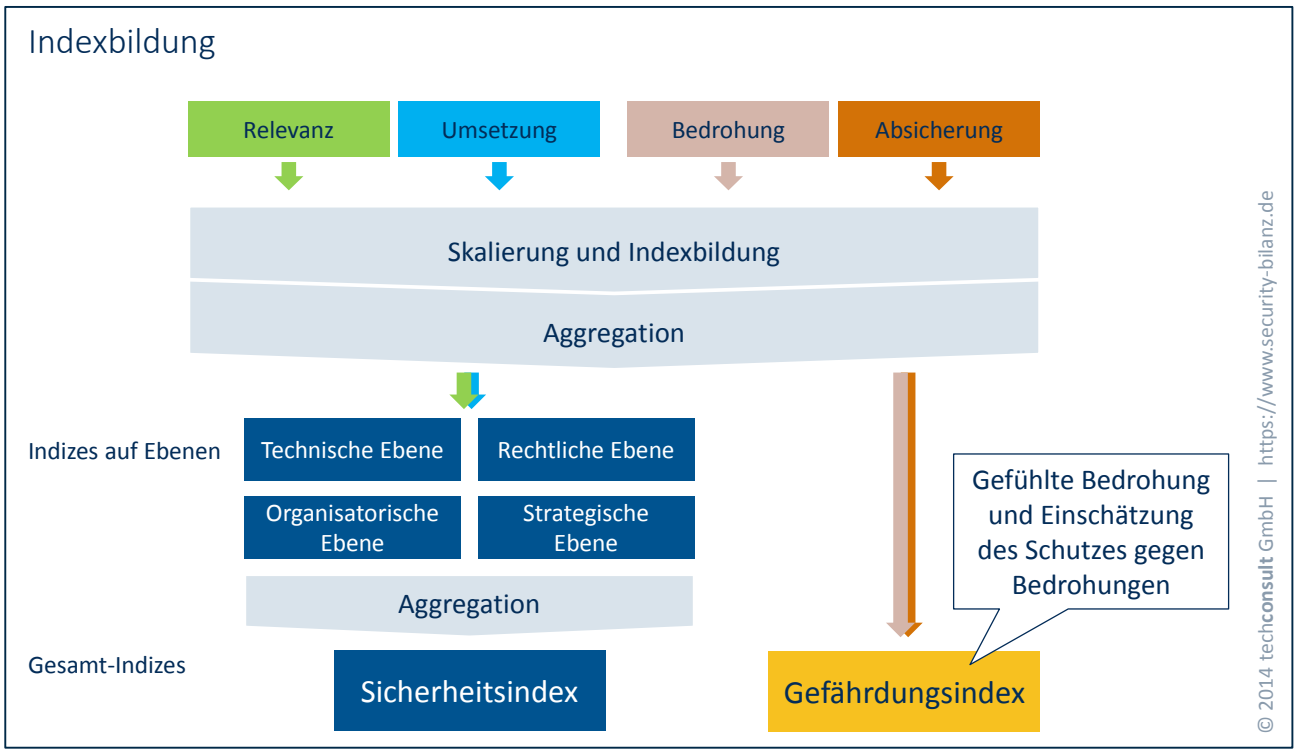

Abbildung 9: Schematische Darstellung der Indexbildung

Kontaktinformationen

ÜBER TECHCONSULT

Die techconsult GmbH, gegründet 1992, zählt zu den führenden Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Die techconsult GmbH wird von den geschäftsführenden Gesellschaftern und Gründern Peter Burghardt und Andreas W. Klein am Standort Kassel mit einer Niederlassung in München geleitet und ist Teil der Heise Medien Gruppe.

tech**consult** GmbH

– The IT Market Analysts –

Am Platz der Deutschen Einheit

Leipziger Straße 35–37

Tel. +49 561 – 8109 -0

Fax +49 561 – 8109 -101

http://www.techconsult.de

Sponsoren

Die baramundi software AG bietet Management-Software für Clients, Server und mobile Geräte. Der Fokus liegt dabei auf sicherem Management von Arbeitsplatzumgebungen, plattformübergreifend und für verschiedenste Endgeräte, sowie auf Compliance- und Schwachstellenmanagement.

Die MESH GmbH bietet maßgeschneiderte Datacenter-, Cloud- und Connectivity-Services für den Mittelstand und unterstützt Unternehmen beim Outsourcing der Infrastruktur in sichere IT-Rechenzentren. Bei den MESH Trusted Cloud Lösungen können zusätzlich Private-, Community- oder Hybrid-Cloud Services individuell betrieben und miteinander kombiniert werden. ISO-zertifizierte Rechenzentren sowie sichere Netzwerkdienste durch Multi-Tier I Carrier-Anbindungen garantieren eine hohe Verfügbarkeit und Ausfallsicherheit.

Die Microsoft Deutschland GmbH richtet sich mit seinem Safety & Security Center mit Sicherheitshinweisen und Hintergrundartikeln an alle IT-Anwender, die ihre IT-Umgebungen schützen wollen. Das Safety & Security Center bietet neben allgemeinen Informationen auch praktische Hinweise, z.B. wie Angriffsversuche zu erkennen und abzuwenden sind.

Die NCP engineering GmbH ist technologischer Weltmarktführer für Lösungen rund um den ferngesteuerten Zugriff auf zentrale Datenbestände und Ressourcen von Unternehmen. NCP liefert Produkte, Spitzentechnologie, zentrales Remote Access Management und End-to-Site Sicherheit „aus einer Hand“.

Die Sophos GmbH hat sich der Sicherheit und dem Schutz aller existierenden Endpoints von Netzwerken verschrieben. Durch individuelle, an Unternehmensanforderungen angepasste Produkte können alle Geräte eines Netzwerks zuverlässig, einfach und zentral in der Cloud verwaltet werden.

Telekom bietet Anwendern komplette IT Sicherheit: beginnend mit Checks und Consulting (IT Security Checks) über umfassende Sicherheit für Unternehmensnetze (Managed Network Security) und volle Sicherheit für feste und mobile IT Arbeitsplätze (Managed Endpoint Security) bis hin zur Sicherheit für sensible Kommunikation und Daten kombiniert (Managed Communication Security).