techconsult
The IT Market Analysts

Unterstützt von Bitdefender ITSECURITY Bavarian IT Security & Safety Cluster

Juni 2016

Market Paper

IT-Sicherheit in Öffentlichen Verwaltungen

Ergebnisse aus der tech**consult** Langzeitstudie **Security Bilanz Deutschland** mit dem Fokus auf öffentlichen Verwaltungen

---

SUMMARY

Öffentliche Verwaltungen weisen in vielen Bereiche deutliche Umsetzungsprobleme im Bereich IT- und Informationssicherheit auf. Das Market Paper untersucht, wie gut die derzeitige Umsetzung im Bereich der technischen Lösungen inkl. Mobile Security von den Verwaltungen selbst bewertet. Darüber hinaus zeigt die Analyse der Einschätzung der Gefährdungslage, dass öffentliche Verwaltungen sich häufig weniger bedroht fühlen als Unternehmen des Mittelstands.

INHALT:

Verfall der IT- und Informationssicherheit in öffentlichen Verwaltungen?

Öffentliche Verwaltungen sind beim Thema IT- und Informationssicherheit bisher nicht gut aufgestellt. Mehr noch: Von Jahr zu Jahr scheint sich eher eine Verschlechterung als eine Verbesserung abzuzeichnen, obwohl das Bewusstsein, dass etwas getan werden muss, insgesamt kontinuierlich zunimmt. Dies ist eine Erkenntnis der Studie Security Bilanz Deutschland, mit der techconsult seit drei Jahren jährlich den Status quo der IT- und Informationssicherheit in Mittelstand und öffentlichen Verwaltungen ermittelt.

Die vielfach mangelhafte Umsetzung von Maßnahmen und Lösungen für IT- und Datensicherheit ist auch bei mittelständischen Unternehmen festzustellen, öffentliche Verwaltungen weisen jedoch noch deutlich häufiger Probleme auf. Dies betrifft alle Ebenen, die dazu beitragen IT- und Datensicherheit sicherzustellen: Dies sind sowohl die technische Umsetzung, als auch organisatorische, rechtliche und strategische Maßnahmen.

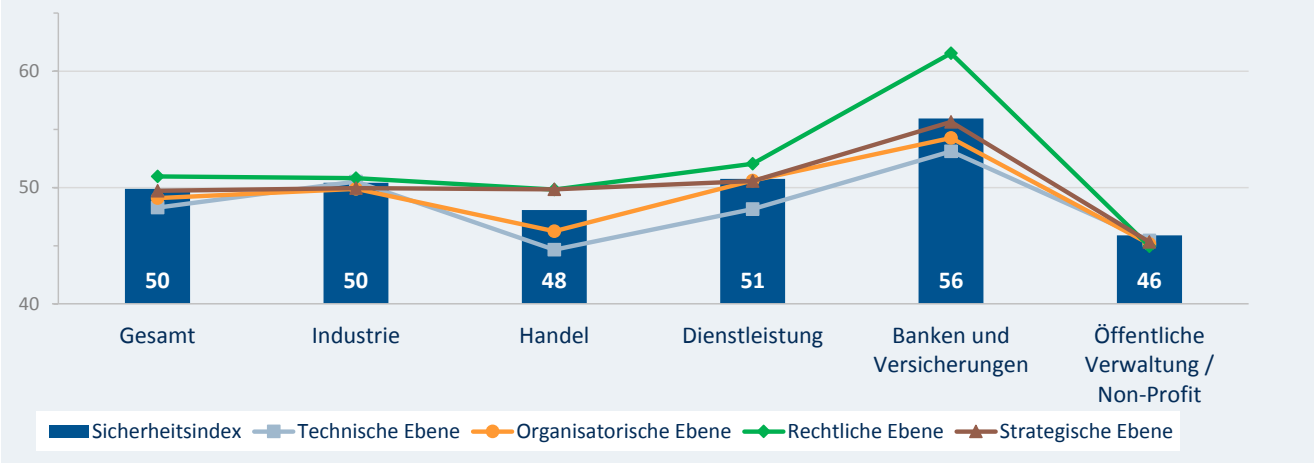

Abbildung 1: Vergleich von Sicherheitsindex und Sicherheitsindizes auf den verschiedenen Ebenen nach untersuchten Branchen

Im Folgenden wird an einigen ausgewählten Lösungsbereichen untersucht, wo bei der technischen IT-Sicherheit Probleme bestehen. Darüber hinaus wird analysiert, wie die Bedrohungslage von öffentlichen Verwaltungen eingeschätzt wird beziehungsweise wie gut sie sich gegen Angriffe abgesichert fühlen.

Umsetzung der technischen IT-Sicherheit in ausgewählten Lösungsbereichen

Die Security Bilanz Deutschland untersucht aus einer ganzheitlichen Perspektive, wie IT- und Informationssicherheit in Unternehmen und Verwaltungen umgesetzt wird. Dabei werden zum einen technische Maßnahmen und Lösungen betrachtet, als auch organisatorische, rechtliche und strategische Maßnahmen, die ergriffen werden. Bei der im Folgenden fokussierten technischen Umsetzung von IT-Sicherheit werden folgende Kategorien von Lösungen unterschieden:

- Lösungen für den Basisschutz,
- Lösungen für die Absicherung von mobilen Endgeräten wie Smartphones und Tablets sowie
- Security Lösungen aus der Cloud

Lösungen für den Basisschutz

Hierunter fallen gängige Lösungen aus den Bereichen Endpoint und Network Security, wie z.B. Antiviren-Lösungen, Firewalls oder E-Mail-Security-Lösungen und Spamfilter. Schon bei diesen vergleichsweise einfach umzusetzenden Basisschutzlösungen bewerten mehr als die Hälfte der Befragten die Umsetzung als nicht gut.

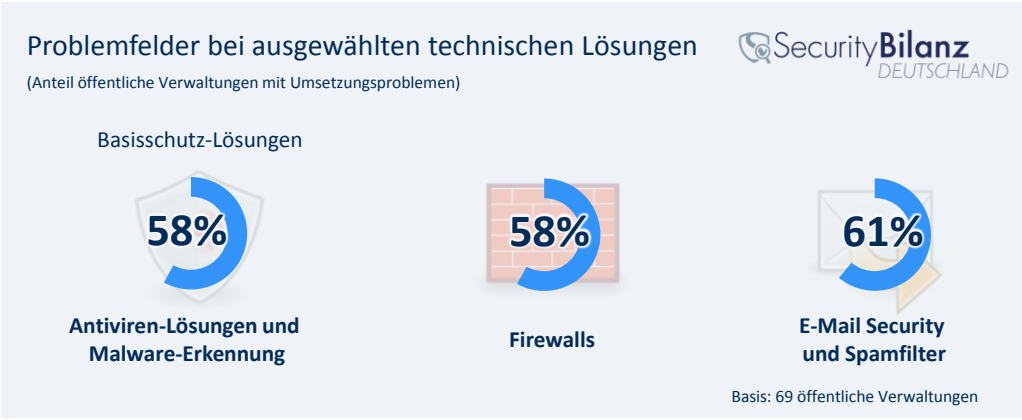

Abbildung 2: Anteil der Unternehmen mit Umsetzungsproblemen bei technischen Lösungen

Antiviren-Lösungen und Firewalls werden von den öffentlichen Verwaltungen zwar wichtiger angesehen als von mittelständischen Unternehmen, trotzdem fällt die Einschätzung der bisherigen Umsetzung dieser Lösungen durchweg

schlechter aus als im privatwirtschaftlichen Sektor. So geben 58 Prozent der öffentlichen Verwaltungen an, dass Antiviren-Lösungen und Malware-Erkennung nicht gut umgesetzt sind. Dadurch ergibt sich deutlich häufiger ein Defizit bei der Umsetzung gegenüber der der jeweiligen Lösung zugemessenen Relevanz. Nicht nur aufgrund des bisher niedrigen Umsetzungsniveaus, sondern auch weil eine höhere Relevanz gesehen wird, das heißt die Anforderungen höher liegen, sollten öffentliche Verwaltungen bei Basisschutzlösungen dringend nachbessern.

Lösungen für die Absicherung von mobilen Endgeräten

Öffentliche Verwaltungen sind im Hinblick auf die Nutzung von mobilen Endgeräten bisher deutlich zurückhaltender als Unternehmen. Doch mit der zunehmenden Digitalisierung und durch Bemühungen, die Attraktivität zu steigern und Bürgern ein besseres Service-Erlebnis zu bieten, werden zukünftig vermehrt mobile Endgeräte wie Tablets und Smartphones in den Amtstuben eingesetzt werden. Darüber hinaus gibt es auch im öffentlichen Sektor Mitarbeiter im Außendienst, die vom Einsatz mobiler Endgeräte profitieren, z.B. im Bereich der Ordnungsämter, der Verkehrsüberwachung, im Bereich der Bauaufsicht oder bei Versorgungsbetrieben.

Die aktuelle Selbsteinschätzung der öffentlichen Verwaltungen hinsichtlich des Sicherheitsniveaus im Bereich Mobile Security zeigt dabei deutlich, dass hier noch großer Nachholbedarf vorhanden ist, was nicht zuletzt auf die bisher geringe Nutzung der Technologie zurückgeführt werden kann. Fast drei Viertel der Befragen bewerten ihre bisherige Umsetzung von Sicherheitsmaßnahmen als problematisch oder gar nicht vorhanden.

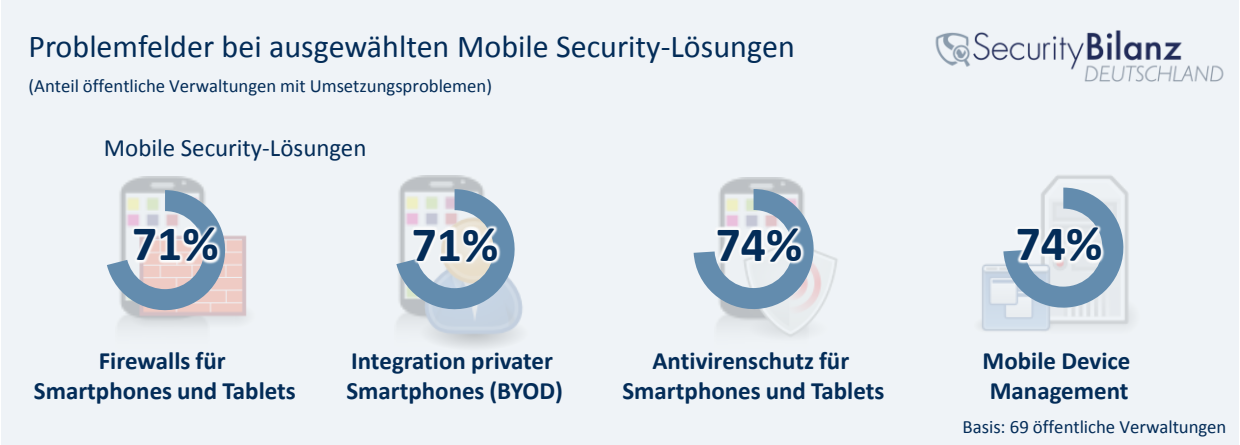

Abbildung 3: Anteil der Unternehmen mit Umsetzungsproblemen bei Mobile Security-Lösungen

Security aus der Cloud: E-Mail & Web Protection

Gerade für kleinere Unternehmen und Behörden können Security as a Service-Lösungen, also Security aus der Cloud, eine sinnvolle Alternative zu on premise betriebenen Lösungen darstellen, weil sich der Aufwand für die IT-Abteilung bei Betrieb und Administration erheblich verringern kann. Auch können solche Lösungen sehr viel besser skaliert werden, weil der Dienstleister, der die Lösung bereit stellt, Ressourcen in sehr viel größerem Umfang bereit stellen kann, als in einem einzelnen Unternehmen in der Regel weder wirtschaftlich abbildbar noch technisch möglich ist, weil auch die übrige Infrastruktur gar nicht dafür ausgelegt ist.

Bei den oben beschriebenen Basisschutzlösungen wurde festgestellt, dass bei 61 Prozent der öffentlichen Verwaltungen Umsetzungsprobleme im Bereich E-Mail-Security und Spamfilter bestehen. Durchschnittlich beziehen bereits rund 50 Prozent aller Befragten (Mittelstand und Verwaltungen) Security-Lösungen für E-Mail und Web Protection aus der Cloud. Im öffentlichen Sektor liegt der Anteil mit rund 52 Prozent schon leicht über dem Durchschnitt.

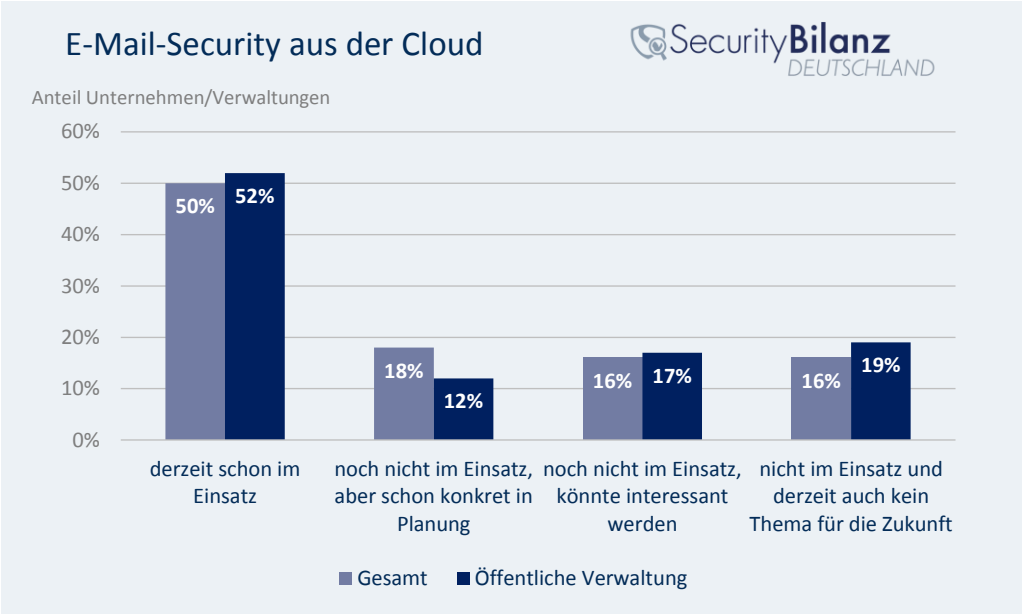

Abbildung 4: Anteil der Unternehmen, die E-Mail-Security aus der Cloud beziehen oder Planungen dazu haben

Konkrete Planungen gibt es nur bei 12 Prozent der öffentlichen Verwaltungen. Im Mittelstandsdurchschnitt ist es fast jedes fünfte Unternehmen, das daran arbeitet E-Mail und Web Protection im Mietmodell zu beziehen. 19 Prozent der Verwaltungen geben an, auch zukünftig keine Cloud-Lösung in diesem Bereich beziehen zu wollen.

Welche Bedrohungen werden gesehen? Wie gut fühlt man sich dagegen geschützt?

Insgesamt zeigt sich die Einschätzung der Bedrohungslage durch die öffentlichen Verwaltungen von Jahr zu Jahr relativ konstant. Der von der Studie ermittelte Bedrohungsindex ist seit dem Studienbeginn 2014 nur leicht von 47 Indexpunkten auf aktuell 48 Punkte angestiegen. Zugleich ist die Bewertung der Umsetzung von Sicherheitsmaßnahmen und -lösungen jedoch kontinuierlich von 50 Indexpunkten im Jahr 2014 auf aktuell 45 Punkte zurückgegangen.

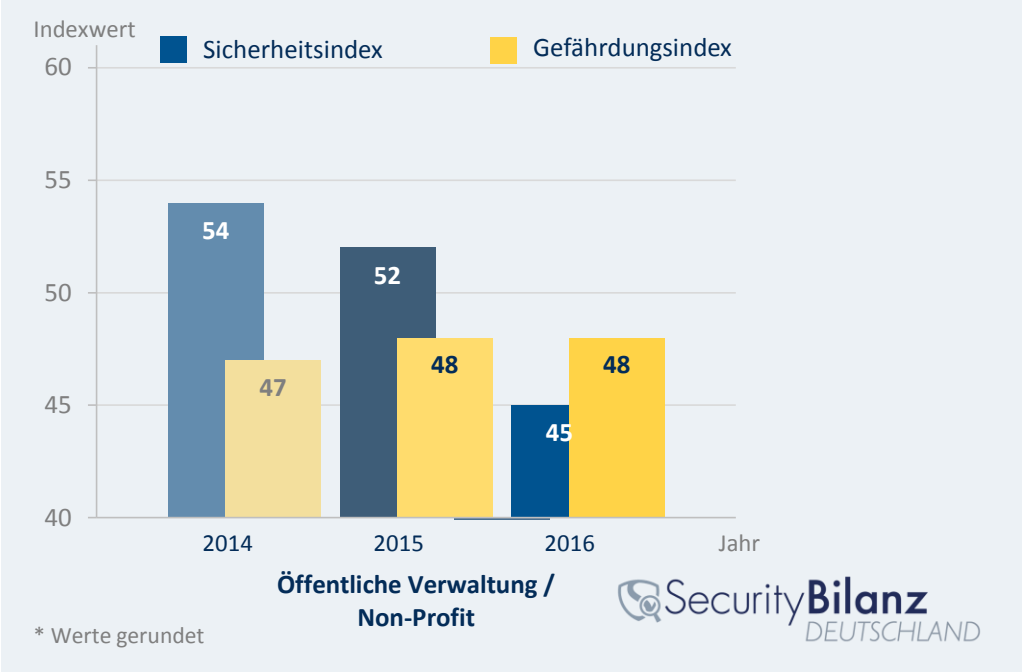

Abbildung 5: Gegenüberstellung von Sicherheitsindex und Gefährdungsindex für öffentliche Verwaltungen

Öffentliche Verwaltungen fühlen sich weniger bedroht als andere Branchen: Nur knapp ein Viertel gab an, im unbefugten Zugang zu Systemen und Daten durch Trojaner, Hackerangriffe oder Spyware eine große oder sehr große Bedrohung zu sehen. Ebenfalls nur knapp ein Viertel sieht Ransomware als eine große oder sehr große Bedrohung an (27,5%). Im Durchschnitt sind es jeweils mehr als ein Drittel der Unternehmen, die sich hiervon bedroht fühlen. Ähnlich gering wird die Bedrohung allenfalls von den Unternehmen des Handels eingeschätzt.

Gleichzeitig sieht sich die Öffentliche Verwaltung aber auch nur unterdurchschnittlich gut geschützt gegen die abgefragten Bedrohungsszenarien. Am

schlechtesten fühlen sich öffentliche Verwaltungen gegen Zielgerichtete Angriffe (Advanced Persistent Threats, APT), Verschlüsselungstrojaner (Ransomware) sowie gegen Angriffe auf mobile Endgeräte und Abhören von Telefonie abgesichert. Jeweils fast drei Viertel der Verwaltungen sehen ihre Absicherung gegen diese Angriffe als problembehaftet an. Wohlgemerkt: Die Befragung erfolgte Anfang 2016, kurz bevor auch im öffentlichen Sektor vermehrt Fälle von Ransomware-Befall bekannt wurden. Insofern kann dieser Befund als Bestätigung angesehen werden, dass öffentliche Verwaltungen hierfür besonders anfällig sind.

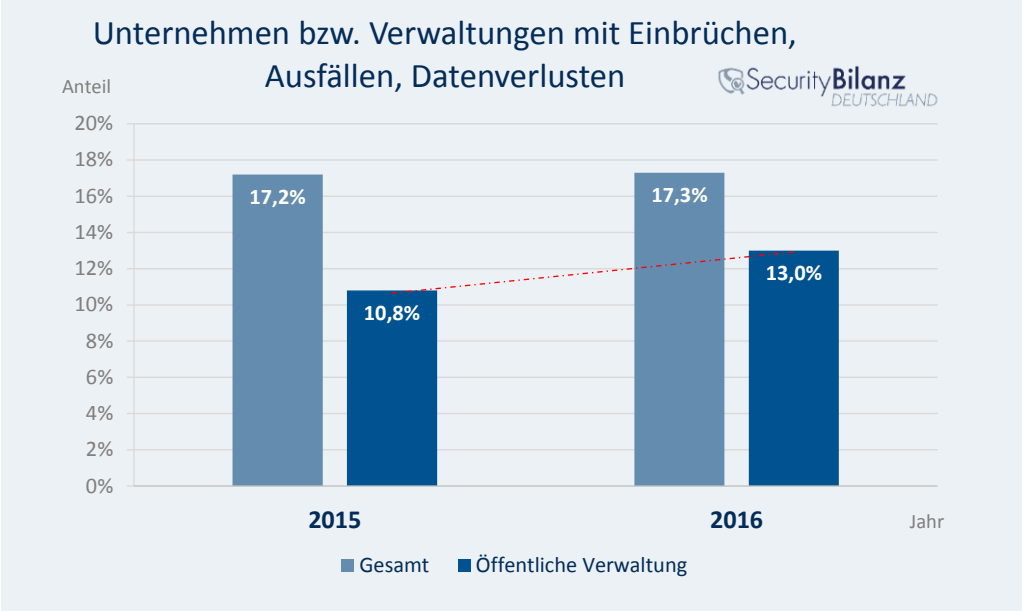

Abbildung 6: Anteil der Verwaltungen, die im vergangenen Jahr einen Ausfall bzw. Ausfälle von IT-Systemen, Einbrüche in IT-Systeme oder Datenverluste erlitten haben

Es erscheint ratsam, die Bedrohungen ernster zu nehmen. Mehr als jede zehnte der befragten öffentlichen Verwaltungen gab an, im vergangenen Jahr einen Einbruch in Systeme bzw. Ausfall von Systemen oder Datenverlust erlitten zu haben. Dieser Anteil liegt zwar unter dem Gesamtdurchschnitt aller untersuchten Unternehmen und Verwaltungen, gleichzeitig ist jedoch ein deutlicher Anstieg von 2,2 Prozentpunkten gegenüber dem Vorjahr festzustellen. Dabei gilt es auch zu bedenken, dass möglicherweise nicht alle Einbrüche oder Datenverluste bemerkt werden – und dass dies in der öffentlichen Verwaltung häufiger der Fall ist, legt die schlechtere Umsetzung von IT-Sicherheitsmaßnahmen und -lösungen nahe.

Fazit

Öffentliche Verwaltungen sind in vielen Bereichen der IT- und Informationssicherheit nicht gut aufgestellt. Ähnlich sieht es auch in mittelständischen Unternehmen aus, doch der öffentliche Sektor weist auf allen Ebenen der Absicherung häufiger Defizite auf als die Privatwirtschaft und hat somit einen gewissen Rückstand, was auch eine stärkere Gefährdung zur Folge hat. Die Bedrohungen werden jedoch noch häufig unterschätzt; beispielsweise sieht nur knapp ein Viertel der Verwaltungen in Ransomware eine große Bedrohung – gleichzeitig fühlen sich jedoch fast drei Viertel nicht gut gegen diese Art von Angriffen abgesichert.

In Hinblick auf die getroffenen Maßnahmen und Lösungen für IT- und Informationssicherheit weisen öffentliche Verwaltungen im Vergleich zum Mittelstand deutlich häufiger Probleme bei der Umsetzung auf. Hier besteht somit noch einiger Handlungsbedarf, zumal davon auszugehen ist, dass die Häufigkeit von Angriffen weiter zunimmt. Weiterhin ist auch im öffentlichen Sektor von einer zunehmenden Nutzung von Mobile Devices auszugehen, die bisher noch zurückhaltend eingesetzt werden. Um das bisher häufig mangelhafte Umsetzungsniveau von Mobile Security-Lösungen zu verbessern, bedarf es noch einiger Anstrengungen, um einen sicheren Einsatz von mobilen Endgeräten zu ermöglichen.

Cloud-Lösungen können ein Mittel sein, ein bisher nicht gut umgesetztes Lösungsbereich deutlich zu verbessern, weil der Aufwand für Betrieb gemessen am zu erzielenden Mehrwert in der Regel geringer ausfällt als bei selbst betriebenen Lösungen. Öffentliche Verwaltungen nutzen diese Bezugsmöglichkeit bei E-Mail und Web Protection schon überdurchschnittlich häufig.

Über die Security Bilanz Deutschland

Die Studie Security Bilanz Deutschland ermittelt jährlich den Status Quo der IT- und Informationssicherheit im Mittelstand und öffentlichen Verwaltungen. Die Basis bildet eine repräsentative Befragung mit über 500 Interviews in Unternehmen und Verwaltungen/Non-Profits mit 20 bis 2.000 Mitarbeitern. Darüber hinaus steht mit dem Heise Security Consulter ein Self-Check-Tool bereit, mit dem Unternehmen und Verwaltungen ihre Lage bewerten und mit den Studienergebnissen vergleichen können. Mehr Informationen und das Self-Check-Tool sind zu finden unter https://www.security-bilanz.de.

Henrik Groß
– Analyst –

tech**consult** GmbH

Baunsbergstr. 37
D-34131 Kassel

Kontakt:

Nancy Weddig
– Presse und Public Relations –

E-Mail: nancy.weddig@techconsult.de
Tel.: +49-561-8109-140
Fax: +49-561-8109-101
Web: www.techconsult.de

Über techconsult

Die tech**consult** GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt tech**consult** 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 tech**consult** GmbH wird vom geschäftsführenden Gesellschafter und Gründer Peter Burghardt am Standort Kassel mit einer Niederlassung in München geleitet und ist Teil der Heise Medien Gruppe.