Whitepaper

WIE „CYBER SECURE" IST DER DEUTSCHE MITTELSTAND?

IT's like you.

SIEVERS GROUP

WIR WOLLEN ES WISSEN: WIE SICHER IST DER DEUTSCHE MITTELSTAND?

01

Hintergrund.

Das Spektrum der Meinungen könnte unterschiedlicher nicht sein, wenn es um Cyber Security geht. Die Medien spiegeln vielfältige Bedrohungen, Anbieter von Security-Lösungen evaluieren permanent Schwachstellen.

Fest steht: Das Gefühl von Sicherheit oder Unsicherheit ist einerseits höchst subjektiv geprägt. Andererseits spüren viele Unternehmen spätestens seit Geltung der Datenschutz-Grundverordnung, dass Informationssicherheit kein rein internes Thema mehr ist. Ein sicherer Umgang mit dem Stand der Technik und der Analyse und Behandlung von Cyber-Risiken wird nicht nur von Aufsichtsbehörden vorausgesetzt. Auch Geschäftspartner, Versicherungen, Banken und Wirtschaftsprüfer verlangen im Zweifel den Nachweis eines angemessenen Sicherheitsniveaus.

Unklar ist dabei oft, was ein angemessenes Sicherheitsniveau ist. Unternehmen stehen also vor der Herausforderung, Bedrohungen und Schwachstellen zu identifizieren, und die sich daraus ergebenden Risiken zu bewerten.

02

Cyber Security Schutzziele.

Die Schutzziele der Cyber Security werden dabei individuell berücksichtigt und ggf. priorisiert:

1) Integrität:
Unter Integrität fallen alle Anforderungen an die Korrektheit (Unversehrtheit) von Informationen bzw. an die korrekte Funktionsweise der Datenverarbeitung.

2) Verfügbarkeit:
Unter Verfügbarkeit fallen alle Maßnahmen, um IT-Ressourcen in der definierten Art und Weise nutzen zu können.

3) Vertraulichkeit:
Unter Vertraulichkeit werden alle Anforderungen zur Beschränkung des Zugangs zu Informationen verstanden.

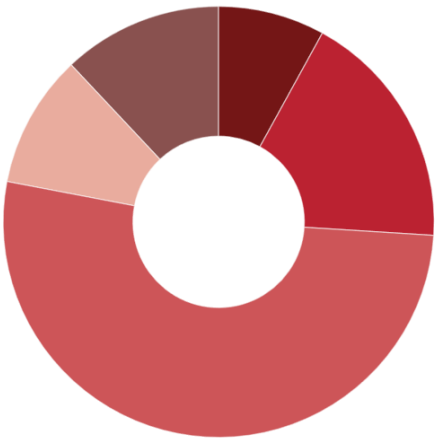
Diese drei Schutzziele stehen also im Mittelpunkt der Cyber Security. Das Niveau der technischen und organisatorischen Maßnahmen wird jedoch auch in gängigen Normen zur Informationssicherheit wie der ISO27001 oder der VDS10000 nicht direkt vorgegeben.

03

Methodik und Zielsetzung.

Wir wollten es genau wissen und haben uns bei mittelständischen Unternehmen umgehört. Wie gehen Unternehmen mit den Bedrohungen um? Welche Erfahrungen liegen vor und was planen Entscheider, um die Unternehmenswerte auch in Zukunft zu schützen? Hier sind die Ergebnisse!

Die Umfrage wurde mittels eines Online-Tools durchgeführt. Die Mehrheit der Umfrageteilnehmer ist dem Segment der kleinen und mittelständischen Unternehmen zuzurechnen *(Vgl. Abb. 1).* Das Befragungstool war zwischen Anfang Oktober und Mitte Dezember frei geschaltet.



bis 9 MitarbeiterInnen	8.0%	10 bis 49 MitarbeiterInnen	18.0%
50 bis 299 MitarbeiterInnen	52.0%	300 bis 1000 MitarbeiterInnen	10.0%
über 1000 MitarbeiterInnen	12.0%		

Abb. 1: Wie viele MitarbeiterInnen hat Ihr Unternehmen?

SUBJEKTIVE SICHERHEIT & TRÜGERISCHE HOFFNUNG BEIM DEUTSCHEN MITTELSTAND

04

Ergebnisse.

70% der Befragten waren noch kein Opfer eines Cyberangriffs *(Vgl. Abb. 2)*. Dieses Ergebnis ist insofern interessant, da ähnliche Befragungen wie z.B. von der Bitkom zu stark abweichenden Ergebnissen gekommen sind.[1] Dort gaben weitaus mehr Unternehmen an, bereits von Cyberangriffen betroffen gewesen zu sein. Aber auch diese Umfrage zeigt, dass knapp jedes vierte Unternehmen schon Opfer eines Cyberangriffs war.

Weiterhin interessant ist die Einschätzung der Unternehmen hinsichtlich ihrer eigenen Sicherheit und die Risikoanalyse. Sicherheit ist subjektiv, Risikoeinschätzungen ebenso. Während 64% der befragten Unternehmen ein generell hohes und damit realistisches Risiko von Cyberangriffen gegen mittelständische Unternehmen in Deutschland sehen, wird das Risiko eines tatsächlichen Angriffs gegen das eigene Unternehmen nur von 28% als hoch bewertet *(Vgl. Abb. 3 und Abb. 4)*.

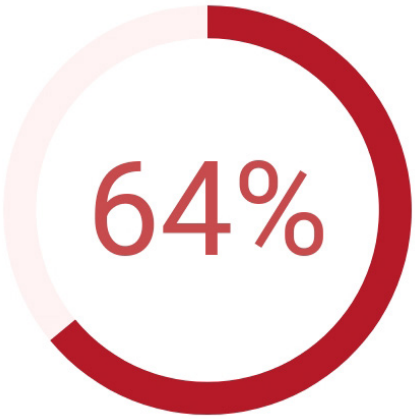


Abb. 4: 64% der befragten Unternehmen sehen ein generell hohes und damit realistisches Risiko von Cyberangriffen

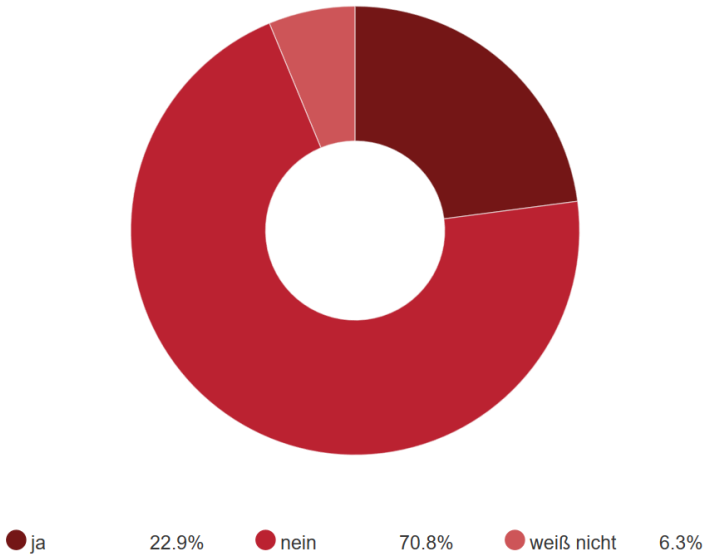


Abb. 2: Wurde Ihr Unternehmen durch Cyberangriffe bereits geschädigt?

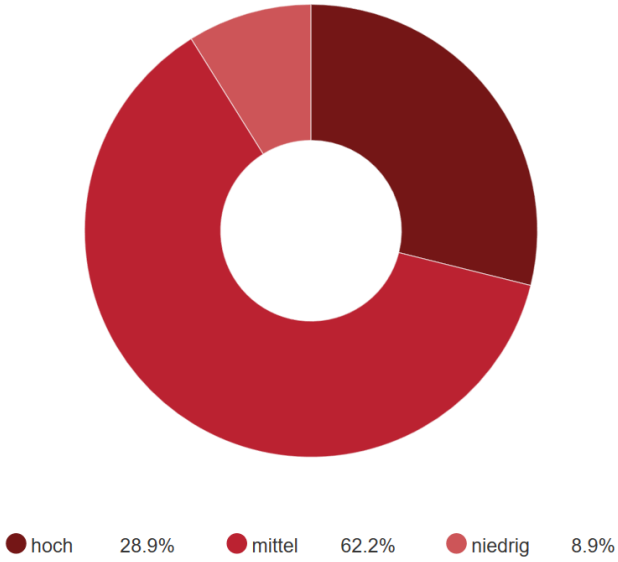


Abb. 3: Das Risiko von Cyberkriminalität für mittelständische Unternehmen in Deutschland ist ...

Konsequenzen eines Cyberangriffs

Für knapp 80% der Befragten wäre ein längerer Ausfall der IT im Unternehmen kritisch oder sogar sehr kritisch. Dennoch stellt sich heraus, dass weniger als die Hälfte der Befragten das eigene Unternehmen als ausreichend geschützt vor Cyberangriffen wahrnimmt. Weitere knapp 25% sind sich diesbezüglich nicht sicher.

Dies bedeutet, dass obwohl Unternehmen das hohe Risiko eines Cyberangriffs anerkennen und ein Ausfall der IT im schlimmsten Fall geschäftsschädigende Konsequenzen mit sich bringen würde, ist der Schutzzustand nicht besonders hoch.

Jedoch haben die meisten Unternehmen bereits einige Sicherheitsmaßnahmen umgesetzt *(vgl. Abb. 5)*. Über Antivirensoftware und Firewall-Systeme verfügt nahezu jedes Unternehmen. Insbesondere im Bereich der Verschlüsslung sensibler Daten gibt es hingegen noch Nachholbedarf, denn laut Angabe verschlüsseln nur 14% der Unternehmen heute ihre sensiblen Daten, welches eine hohe Sicherheitslücke darstellt.

Es gibt noch viel Verbesserungspotential bei Cyber Security-Maßnahmen. Allerdings besteht auch eine hohe Investitionsbereitschaft bei den befragten Unternehmen, denn IT-Sicherheit ist ein Moving-Target. Knapp 90% der Unternehmen werden auch in den kommenden Jahren stetig in ihre IT-Sicherheit investieren.

55%

machen regelmäßige Wiederherstellungs-Tests

88%

der Befragten geben ihren Mitarbeitern einen eigenen, passwortgeschützten Zugang

97%

nutzen Virenscanner und Firewalls und machen systematische Backups

90%

installieren automatisch Sicherheitsupdates

33%

verschlüsseln ihre sensiblen Daten

69%

der Befragten verbieten die Nutzung privater Geräte (z.B. Smartphones) in der Unternehmens-IT

48%

der Befragten haben eine Leitlinie für die Informationssicherheit

Abb. 5 Welche Sicherheitsmaßnahmen werden im Mittelstand bereits umgesetzt?

Organisation und Nachweis der Informationssicherheit

Managementsysteme helfen, die Informationssicherheit in der Struktur des Unternehmens oder der Organisation zu verankern. 60% der befragten Unternehmen setzen heute noch kein Managementsystem für Informationssicherheit ein.

Allgemeinbekannte Informationsmanagementsysteme, wie der BSI Grundschutz, die ISO27001 oder die VdS3473 (inzwischen umbenannt in VdS10000) werden nur selten angewandt. *(Vgl. Abb. 6).*

Wirtschaftsprüfer, Aufsichtsbehörden, Banken, Kunden: Immer dann, wenn Dritte Informationen über die Informationssicherheit anfordern, ist ein Nachweis über die vorhandene Cyber Security hilfreich. Die Mehrheit der befragten Unternehmen verfügt heute noch nicht über ein dokumentiertes IT-Sicherheitskonzept. *(Vgl. Abb. 6).*

EU-DSGVO/GDPR

Seit dem 25. Mai 2018 ist die neue EU-DSGVO in Kraft getreten und verschärft dadurch die Gesetze für Datenschutz in Unternehmen.

Vor allem die TOMs (Technische und organisatorische Maßnahmen) gilt es im Rahmen der Erfüllung der EU-DSGVO sicherzustellen und zu dokumentieren. Die TOMs dienen dazu, personenbezogene Daten nach Art. 5 und Art. 32 EU-DSGVO zu schützen. Jede einzelne Maßnahme (z.B. wie die Vertraulichkeit sichergestellt wird) ist zu dokumentieren. Dieser Vorgang ist sehr zeitaufwändig und fehleranfällig. Ein umgesetztes Cyber Security-Konzept vereinfacht diesen Vorgang extrem, da lediglich auf dieses Konzept verwiesen werden muss.

In fast allen befragten Unternehmen befindet sich die EU-DSGVO noch in der Umsetzungsphase. Dies gilt offenbar auch für die technischen Maßnahmen zur Informationssicherheit. *(Vgl. Abb. 8).*

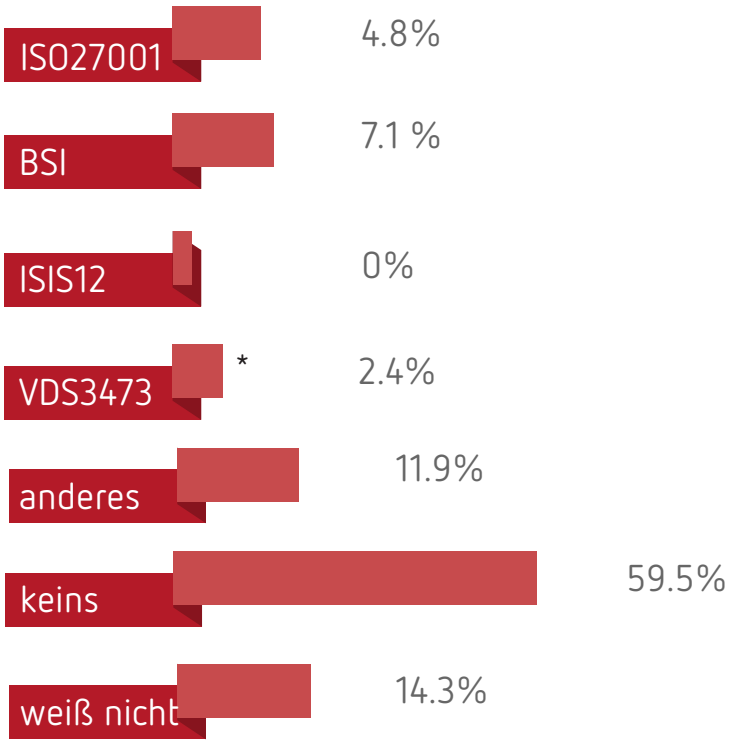


Abb. 6 Nutzen Sie heute schon eines dieser Managementsysteme für Informationssicherheit?

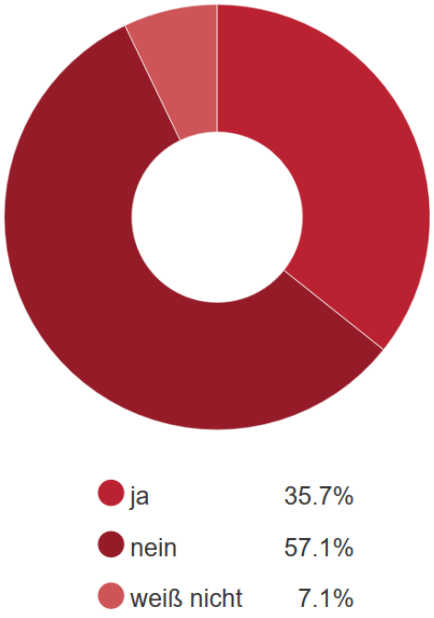


Abb. 7: Haben Sie ein dokumentiertes IT-Sicherheitskonzept?

Abb. 8: Haben Sie die Anforderungen der EU-DSGVO in Bezug auf die Informationssicherheit bereits umgesetzt?

* Die VDS 10000 ist der direkte Nachfolger der VDS3473.

CYBER SECURITY IST IM MITTEL-STAND NOCH NICHT AUF EINEM HOHEN NIVEAU.

04

Fazit.

Zuerst die gute Nachricht: Die Teilnehmer der Umfrage verzichten nicht auf klassische IT-Security-Maßnahmen. Zudem ist klar, dass sich Bedrohungen und Schwachstellen dynamisch entwickeln. Unternehmen reagieren darauf mit kontinuierlichen Investitionen in die Sicherheit der IT.

In den Managementsystemen der Unternehmen spielt das Thema Informationssicherheit jedoch vielfach noch keine Rolle. Hieraus kann erörtert werden, dass die Diskussion um Bedeutung und Schutzziele der Informationssicherheit (gerade im Mittelstand) erst am Anfang steht. Im Zuge der Anpassung an die Datenschutz-Grundverordnung (DSGVO) – die vielfach noch nicht abgeschlossen ist – wird hier ein grundlegender Wandel vermutet.

Gerade für mittelständische Unternehmen mit bereits grundlegender IT-Security kann ein Blick auf bekannte Normen wie die VDS10000 helfen, um nun auch noch die organisatorischen Voraussetzungen zu schaffen, um mit zukünftigen Bedrohungslagen Schritt zu halten. Daraus ergibt sich dann auch ein Fahrplan, wie die Geschäftsführung in die Gesamtverantwortung für Informationssicherheit eingebunden werden kann und wie entsprechende Nachweise gegenüber Dritten erbracht werden können.

Sie möchten mehr über
Cyber Security erfahren?

Dann sprechen sie mich an.
Ich berate sie gerne.

Stefan Ohlmeyer
Berater & IT- Architekt
SIEVERS-GROUP

Tel: 0541 9493-1212
hallo@sievers-group.com