8MAN

Access Rights Management. Only much Smarter.

TRENDREPORT
ACCESS RIGHTS MANAGEMENT IN 2016

Protected Networks

Sehr geehrte Leserinnen und Leser,

in Zeiten elektronischer Geschäftsprozesse und weltweiter Vernetzung ist die effiziente und effektive Nutzung moderner Informationstechnologie genauso wichtig für den Erfolg eines Unternehmens wie Innovationen, wettbewerbsfähige Produkte oder Dienstleistungen und motivierte Mitarbeiter. Informationstechnologie kann jedoch nur dann zum Erfolg beitragen, wenn sie verlässlich arbeitet, oder allgemeiner „sicher" ist. Ein Hauptaugenmerk wollen wir hier auf den Aspekt Schutz von Unternehmensdaten - das **„Gold der digitalen Ära"** - legen.

In seiner Rolle als Innovationstreiber, der lösungsorientiert neue Access Rights Management Produkte in den Markt trägt und so zum Erfolg von Unternehmen entscheidend beiträgt, führt 8MAN jedes Jahr auf der wichtigen IT-Messe CeBIT eine Trendstudie durch. Dieses Jahr hat 8MAN in dieser Studie den Ist-Zustand der Sicherheit bei rund 100 IT-Experten beim Umgang mit Daten und Zugriffsrechten abgefragt und analysiert. Die Studie zeigt einen Statusbericht und verweist auch auf deutliche Verbesserungspotenziale und Handlungsempfehlungen.

Auch vor dem Hintergrund eines zentralen Berechtigungsmanagement-Konzepts dient der Trendreport 8MAN Partnern und Kunden als Richtschnur und Planungshilfe. Im Anschluss an die Zusammenfassung zentraler Erkenntnisse erhalten Sie eine vereinfachte Darstellung der Fragen, Antworten und Zahlen als Grafiken. Inhalt und Aufbau der Studie können zur Selbstanalyse, zur Verbesserung der IT-Sicherheit und damit auch zur Sicherung von Geschäftsprozessen und des Unternehmenserfolgs verwendet werden.

Wir wünschen Ihnen eine aufschlussreiche Lektüre.

Stephan Brack
CEO

Matthias Schulte-Huxel
CSO

Trendreport Access Rights Management in 2016

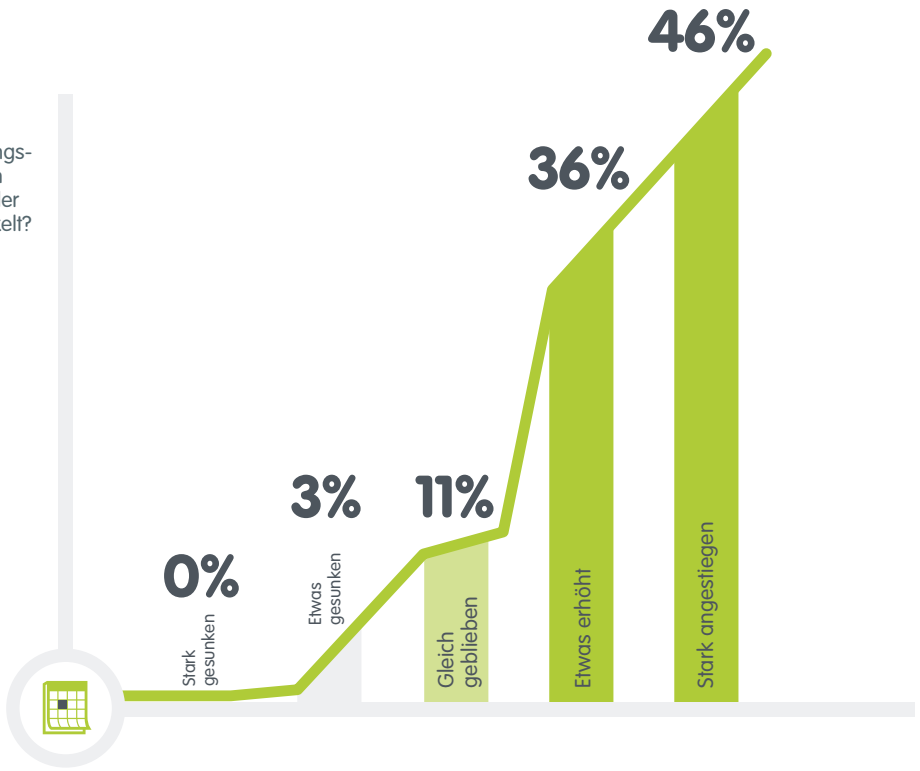
Im Rahmen der Studie „**Access Rights Management Report 2016**" befragte 8MAN rund 100 IT-Experten auf der IT-Fachmesse CeBIT zum Umgang mit Unternehmensdaten und Berechtigungen. Die detaillierten Ergebnisse über die Bedrohungslage, Einsatz und Akzeptanz von Sicherheitsvorkehrungen des Trendreports belegen großes Unwissen und Sorglosigkeit in Unternehmen. Das Studienfazit lautet: IT-Security ist eine Gleichung mit vielen Unbekannten, denn bei vielen Unternehmen ist die IT-Sicherheit unzureichend in die Geschäftsabläufe integriert, um sich effektiv vor Cyberangriffen von außen und innen zu schützen. Dabei sind Datenschutz und Sicherheit der IT-Infrastrukturen gleichbedeutend mit dem Wert einer Firma und damit entscheidend für den Unternehmenserfolg.

Mission Critical: So steht es um die IT-Bedrohungslage

Einig sind sich 46 Prozent der Interviewpartner darin, dass die Bedrohungslage in der Unternehmens-IT in den letzten 12 Monaten stark zugenommen hat. Deutlich gestiegen ist in den vergangenen 12 Monaten das generelle Grundverständnis zur IT-Bedrohungslage, finden 36 Prozent.

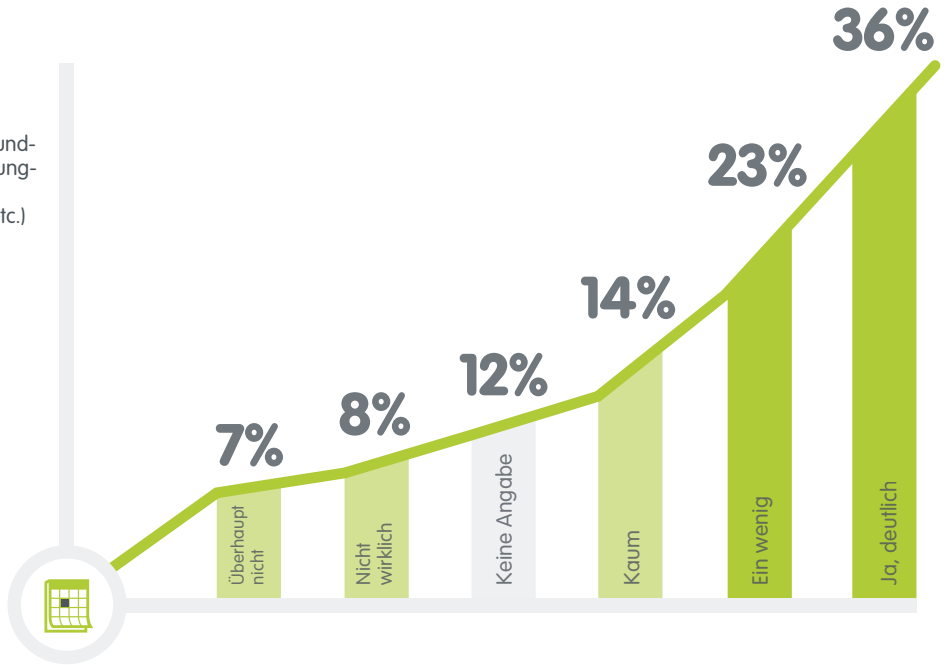
Frage:

Wie hat sich die Bedrohungslage für die IT-Sicherheit in Unternehmen innerhalb der letzten 12 Monate entwickelt?



Frage:

Ist in den vergangenen 12 Monaten generell das Grundverständnis zur IT-Bedrohungslage gewachsen? (z. B. Hacker, Datendiebstahl, etc.)

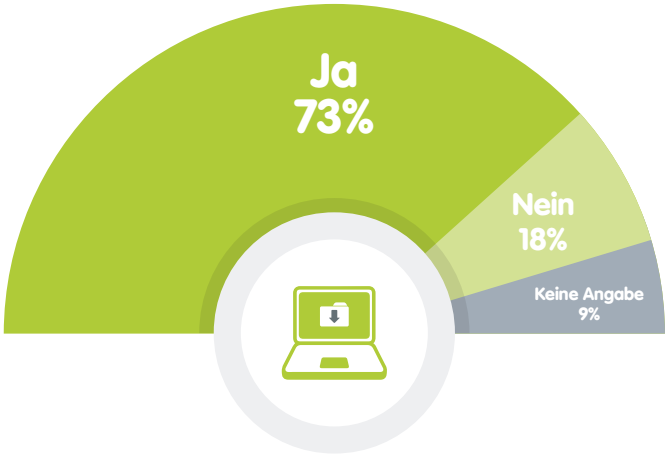


Über den Reifegrad der Informationssicherheit

Für überwältigende 73 Prozent ist der Wert ihres Unternehmens an die IT sowie die Daten auf den verschiedenen Laufwerken gekoppelt. Allerdings werden in 62 Prozent der Unternehmen die Daten nicht einmal nach Vertraulichkeit klassifiziert. Für die Vergabe von Zugriffsrechten ist nur der Administrator zuständig und nicht die Fachabteilung, sagen 86 Prozent. Jedermann-Zugriff sei bei ihnen an der Tagesordnung, erklärten ganze 28 Prozent.

Frage:

Ist die IT-Infrastruktur sowie der Datenbestand in Ihrem Unternehmen unmittelbar mit dem wirtschaftlichen Wert der Firma verbunden? (durch gespeicherte Patente, Konstruktionspläne, etc.)

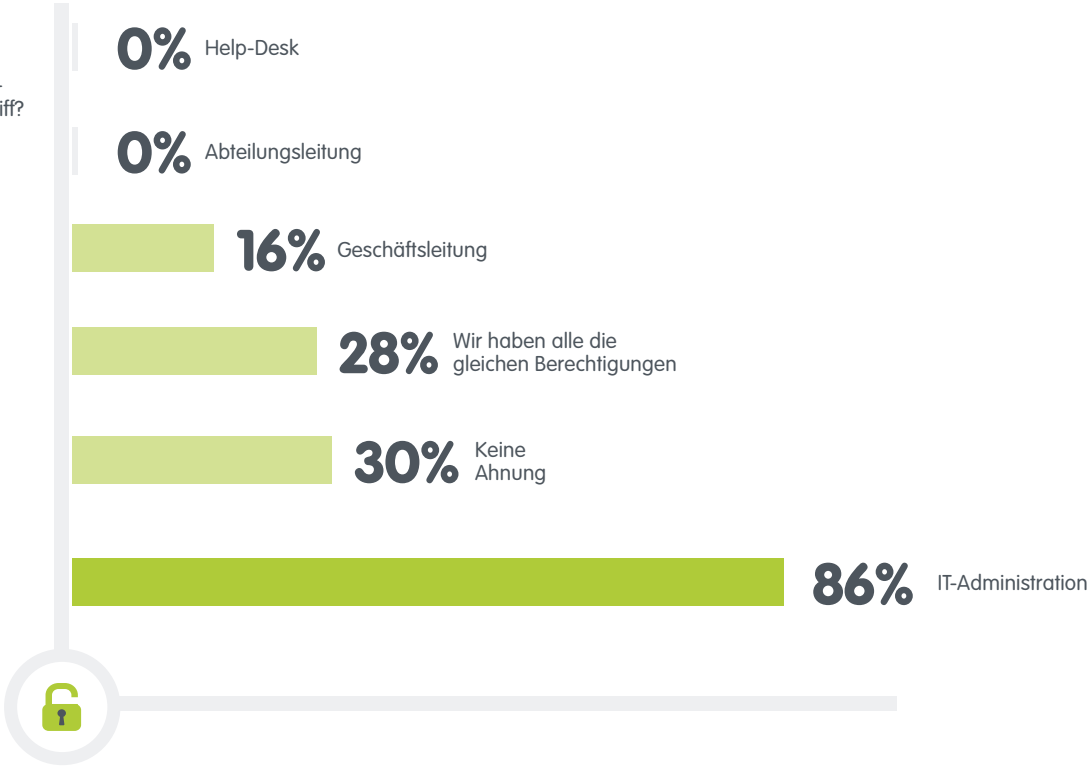


Frage:

Wie klassifiziert Ihr Haus Daten bezüglich ihrer Vertraulichkeit (z.B. alsgeschäftskritisch, vertraulich, Verschlusssache usw.)?

Frage:

Wer vergibt bei Ihnen im Unternehmen die Berechtigungen für den Datenzugriff? (max. 2 Antworten)

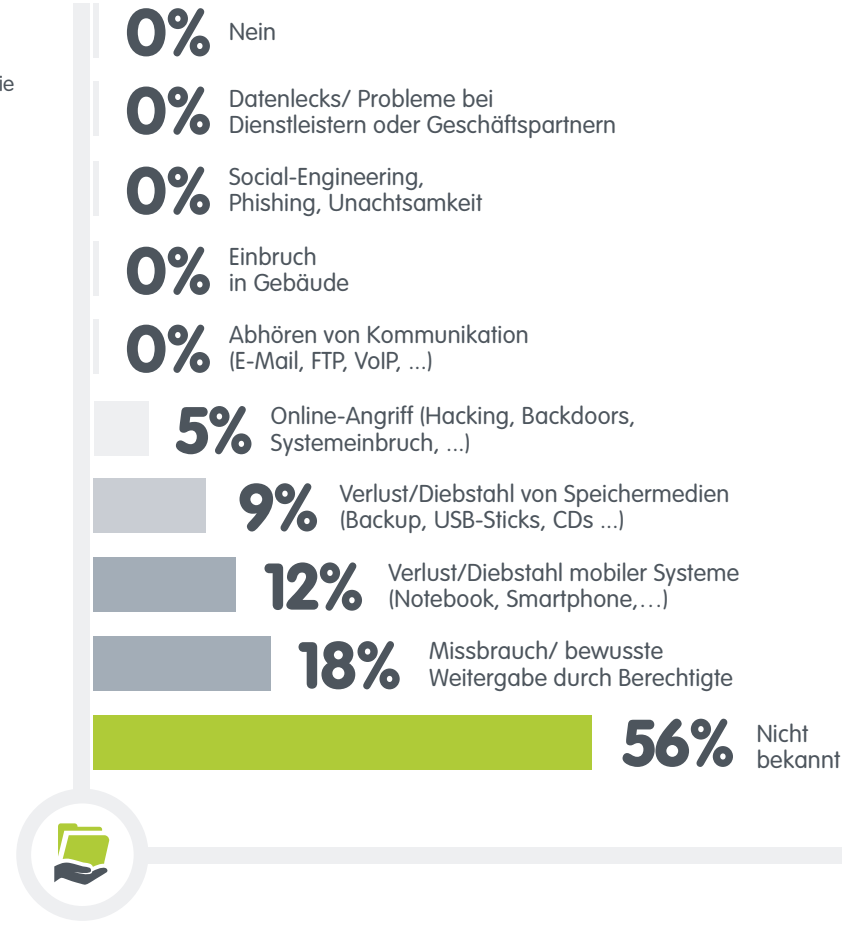


Spannungsfeld Datenzugriff: Potentielle Sicherheitslücken

Bei 56 Prozent der Befragten ist Datenmissbrauch im eigenen Unternehmen nicht bekannt. Wenn Unbefugte Zugriff auf zu schützende Daten erlangten, meinen 18 Prozent, es handle sich dabei um Missbrauch bzw. bewusste Weitergabe aus den eigenen Reihen. 67 Prozent der Befragten sehen auch eine Mitverantwortung für Datenlecks bei den Mitarbeitern.

Frage:

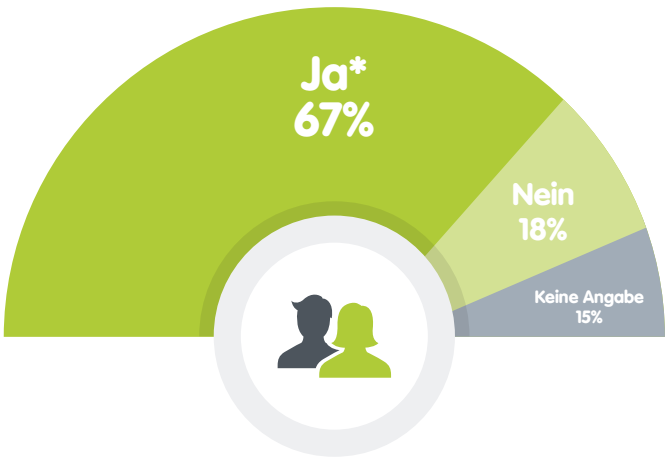
Haben Unbefugte in Ihrem Unternehmen 2014/2015 über die folgenden Wege Zugriff auf zu schützende Daten erlangt?



Frage:

Können Ihrer Meinung nach auch eigene Mitarbeiter eine Mitverantwortung für Datenlecks tragen?

Falls ja: Was sind die Gründe dafür? (Mehrfachantworten erlaubt)

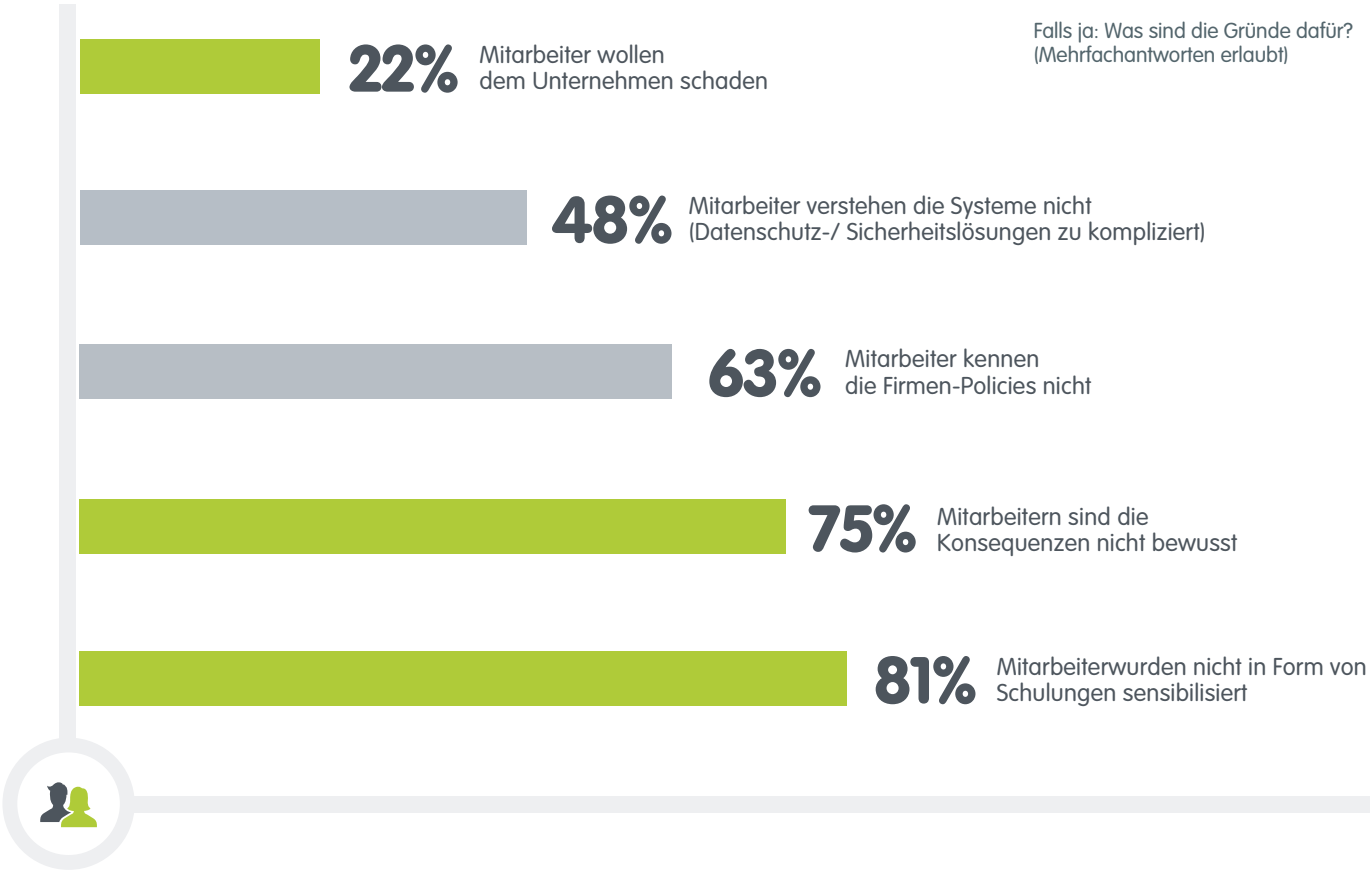


Für 75 Prozent ist klar, dass kaum Konsequenzen beim Ausspähen verbotener Daten drohen. Dabei ist für 22 Prozent ein bewusstes Schaden des Arbeitgebers - beispielsweise im Falle einer Bewerbung bei anderen Marktbegleitern – denkbar. Ganze 63 Prozent gaben an, dass die eigenen Firmen-Policies unbekannt seien.

Frage:

Können Ihrer Meinung nach auch eigene Mitarbeiter eine Mitverantwortung für Datenlecks tragen?

Falls ja: Was sind die Gründe dafür? (Mehrfachantworten erlaubt)

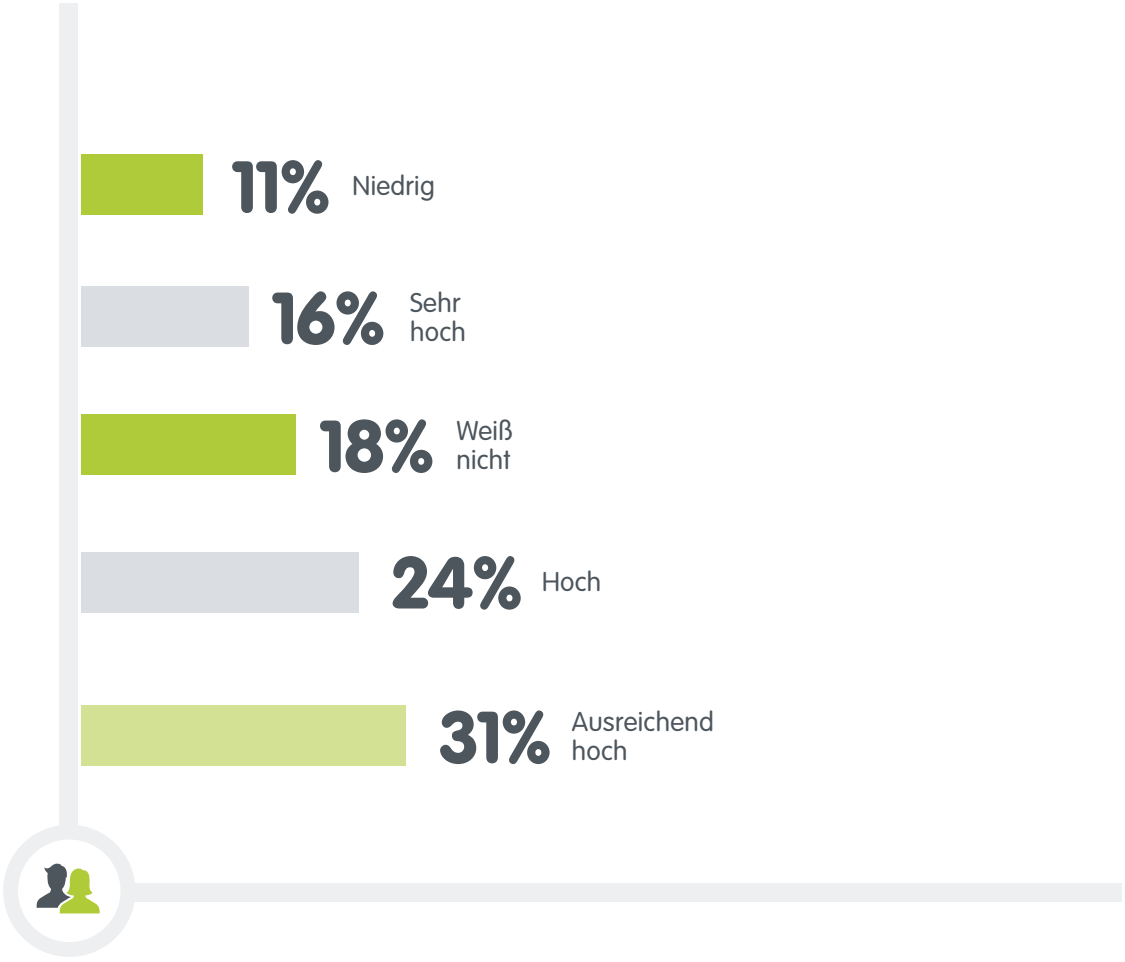


Faktor Mensch: Unternehmen für Gefahren sensibilisieren

Wenn Firmen-Policies weitestgehend unbekannt sind und sich Mitarbeiter der Konsequenzen beim Ausspähen von Daten nicht bewusst sind, verwundert es nicht, dass nur 16 Prozent finden, die Mitarbeitersensibilität sei sehr hoch.

Frage:

Wie hoch ist die Sensibilität bei Mitarbeitern in Unternehmen gegenüber notwendiger IT-Sicherheit?

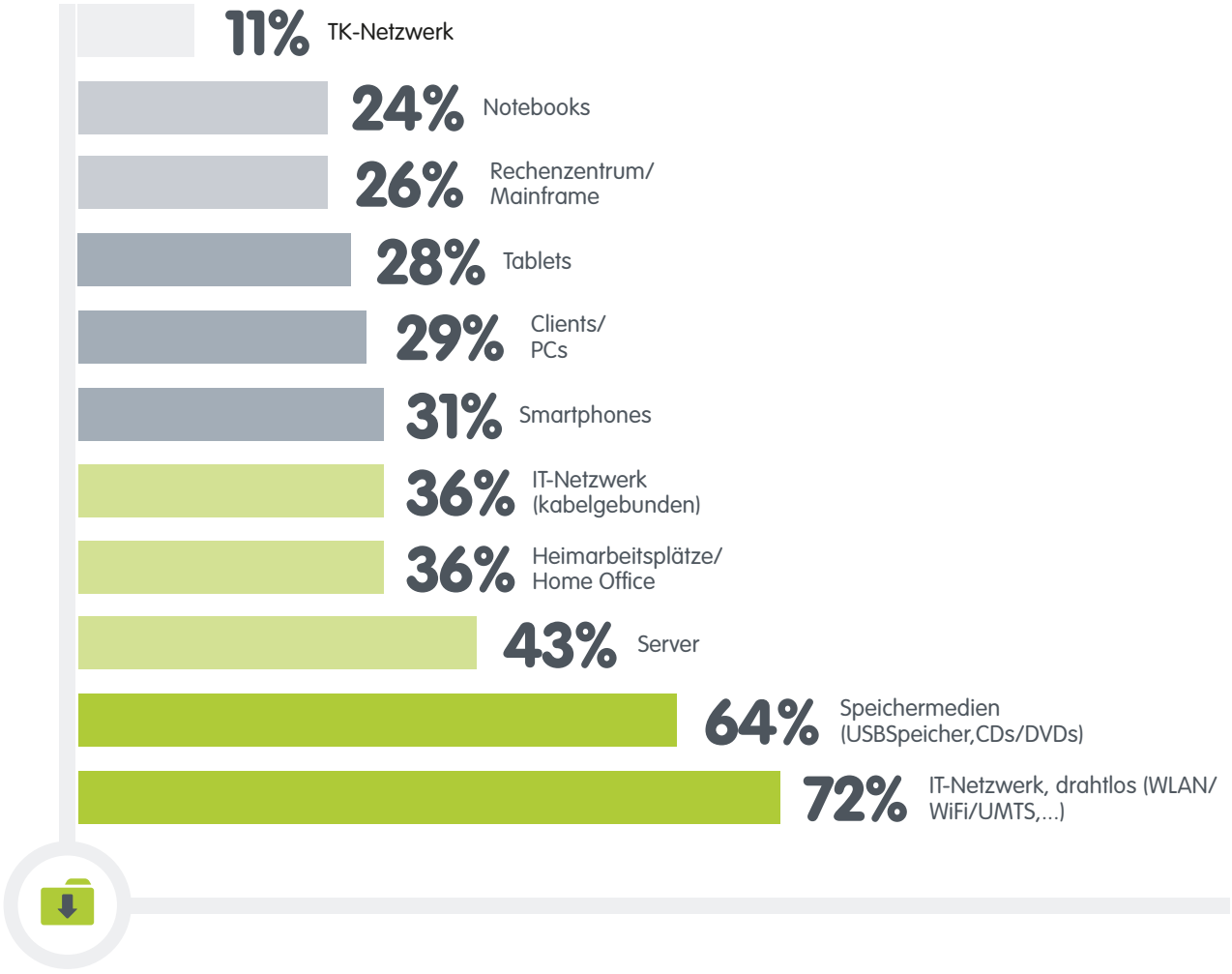


Verlust digitaler Kronjuwelen durch mangelhaftes IT-Management und Sicherheitslecks

Es überrascht nicht, dass für 64 Prozent Speichermedien - USB-Speicher und CDs/ DVDs – das größte Risiko für unbemerkte Datenverluste darstellen.

Frage:

Welche Angriffsstelle bietet das größte Risiko für unbemerkte Datenverluste und Zugriffe? (max. 2 Antworten)

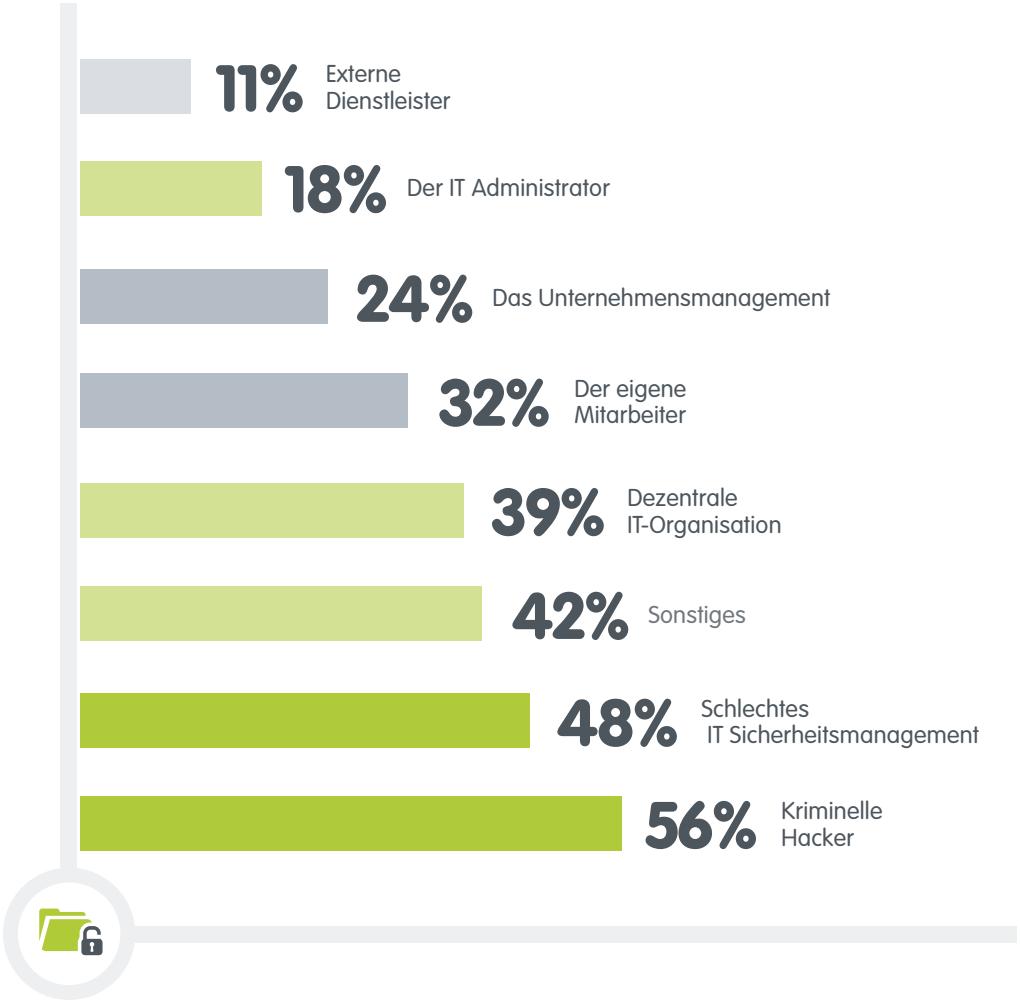


Frage von Schuld und Verantwortung im Unternehmen

Für 48 Prozent ist klar, dass schlechtes IT Sicherheitsmanagement die größte Verantwortung für Datenklau und Datenmissbrauch im Unternehmen trägt. Erst dann, glauben 32 Prozent, ist es der eigene Mitarbeiter.

Frage:

Was vermuten Sie: Wer trägt heute die größte Verantwortung für Datenklau und Datenmissbrauch im Unternehmen? (max. 2 Antworten)



Fazit und Handlungsempfehlung

Die Zusammenfassung der 8MAN Studie zeigt, eine zentrale Instanz für IT-Sicherheit und den Wert eines Unternehmens ist **„wer darf was in den IT-Systemen"**. Das heisst, Berechtigungsverwaltung ist zu einer wettbewerbssichernden Disziplin geworden. Diese betrifft vor allem Unternehmen mit sehr komplexen IT-Systemen und hohen Sicherheitanforderungen sowie Compliancestandards. Mit Cloud, BYOD, Consumerization der IT, Mobility und Industrie 4.0 steigen die Komplexität und die Anforderungen an die Informationstechnologie weiterhin massiv an. Dabei Sicherheit gewährleisten trotz sinkender Budgets und einer dünnen Personaldecke ist eine ständige Herausforderung für Unternehmen. Mit dem richtigen Access Rights Managements (ARM) kann die Sicherheit der IT-Infrastruktur und Unternehmensdaten gewährleistet und dabei sogar die Produktivität gesteigert werden.

Was können Unternehmen also heute schon für Datenschutz und Netzwerksicherheit tun? Zu allererst den Schutz von innen erhöhen, indem sie sich vor unberechtigten Zugriffen auf sensible Daten schützen und die internen Schwachstellen proaktiv und nicht reaktiv beheben. Dabei sind die wesentlichen Merkmale eines wirksamen Berechtigungsmanagements: klare Regelungen treffen, nicht autorisierte Zugriffe und Datenmissbrauch vorbeugen, finanzielle Schäden und Imageverlust minimieren und Prozesse optimieren.

8MAN

Protected Networks GmbH
Alt-Moabit 73
10555 Berlin
Germany

+49 30 390 63 45 - 0
info@8man.com
www.8man.com
www.protected-networks.com