COMPUTERWOCHE CIO ChannelPartner TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE IDENTITY- & ACCESS-MANAGEMENT 2017

PLATIN-PARTNER

procilon GROUP

TIMETOACT GROUP SOFTWARE & CONSULTING

SILBER-PARTNER

AIRLOCK by ergon

NEVIS

BRONZE-PARTNER

Centrify THE BREACH STOPS HERE

KEYIDENTITY

PLATIN-PARTNER

procilon GROUP

TIMETOACT GROUP SOFTWARE & CONSULTING

SILBER-PARTNER

AIRLOCK by ergon

NEVIS

BRONZE-PARTNER

Centrify THE BREACH STOPS HERE

KEYIDENTITY

Studie
IDENTITY & ACCESS MANAGEMENT

Ein aktuelles Studienprojekt von

IDG RESEARCH SERVICES

Platin-Partner

PROCILON GROUP

TIMETOACT GROUP
SOFTWARE & CONSULTING

Silber-Partner

AIRLOCK by ergon

NEVIS

Bronze-Partner

Centrify
THE BREACH STOPS HERE

KEYIDENTITY

WER IST WER in der digitalen Welt? Und: Wie viele?

Diese Fragen beschäftigen uns heute nicht nur im professionellen Kontext. Im Zeichen multipler, digitaler Persönlichkeiten, „Fake News" und „Alternativer Fakten" wird das Vorhandensein einer abgesicherten Identität zum Schlüsselfaktor geschäftlichen Handelns. Umso mehr, als klar ist, dass Kollaboration über traditionelle Grenzen von Unternehmen und abgesicherten Infrastrukturen hinweg eine erfolgskritische Selbstverständlichkeit geworden ist.

Michael Beifuß, Verlagsleiter

Wer wollte auf die digitale Nähe zu seinen Kunden und Geschäftspartnern noch verzichten? Wie soll Wachstum erreicht werden – ohne Teamplay? Aber gleichzeitig muss natürlich auch die Frage beantwortet werden: Wie lassen sich Offenheit, Kollaboration und Partizipation mit Sicherheit, Compliance und Risikomanagement in Einklang bringen?

An der Schnittstelle dieser Welten steht das Identity- & Access-Management (IAM).
Wir freuen uns, dass knapp 400 hochrangige Unternehmensentscheider ihre Erfahrungen und Perspektiven durch die Teilnahme an dieser Studie mit Ihnen teilen. Es zeigt sich, dass der CIO und seine Mannschaft die stärksten Verbündeten für einen softwaregestützten Zugang zum Thema Identity- & Access-Management sind. Hier ist das Bewusstsein über die Herausforderungen und das Machbare am stärksten ausgeprägt.

Klar wird auch: IAM ist nicht gleich IAM.
Es zeigen sich große Unterschiede beim Einsatz der Technologien: Multi-Faktor-Authentifizierung oder das Single-Sign-On bieten noch großes Wachstumspotenzial. Und nicht zu vergessen: Mit der bevorstehenden Einführung der EU-weiten Datenschutz-Grundverordnung steht Informationssicherheit erneut ganz oben auf der Agenda der IT- und Sicherheitsplanungen der Unternehmen. Auch das beleuchtet die vorliegende Studie.

Keine Digitalisierung ohne Sicherheit.
Aber mit Sicherheit auch keine Zukunft ohne Sicherheit. Zugegeben: Diese Aussage ist etwas verkürzt. Aber dennoch: In diesem Spannungsfeld kommt dem IAM eine Schlüsselrolle als „Möglichmacher" der sicheren, kunden- und anwenderorientierten Transformation von Unternehmen zu.

Wir freuen uns über Ihr Interesse an unserer Studie und wünschen Ihnen interessante Einblicke.

Ihr Michael Beilfuß

Inhalt

Management Summary

Die Key Findings im Überblick

Gefahr von außen

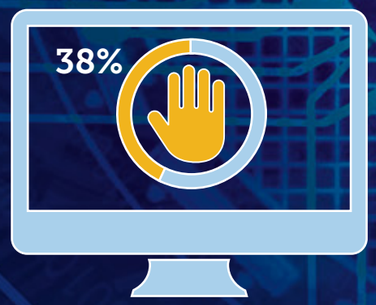
38 Prozent der Unternehmen sehen die externe Bedrohungslage als größte Herausforderung für ihre IT-Security, gefolgt von einem zu geringen (IT-)Security-Budget.

Compliance-Herausforderung Nummer 1

Die EU-Datenschutz-Grundverordnung tritt am 25. Mai 2018 in Kraft. 40 Prozent der Firmen sehen sich davon (sehr) stark betroffen.

Unsicherer Zugang

21 Prozent der Unternehmen sichern ihre Zugänge zum Netzwerk NICHT über eine Multi-Faktor-Authentifizierung mit Token (Hardware, Software oder Push) ab.



Nachholbedarf

Derzeit setzen nur 38 Prozent der befragten Firmen eine Softwarelösung für Identity- & Access-Management (IAM) ein. Vorreiter sind die großen Unternehmen.

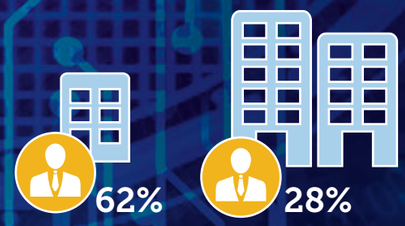
Externe IAM-Dienstleister sind gefragt

59%

Das Gros der Unternehmen arbeitet beim Thema IAM mit einem oder mehreren externen Partnern zusammen.

Ohne Passwort läuft nichts

Das Passwort ist und bleibt mit Abstand die wichtigste Methode im Rahmen der Multifaktor-Authentifizierung.



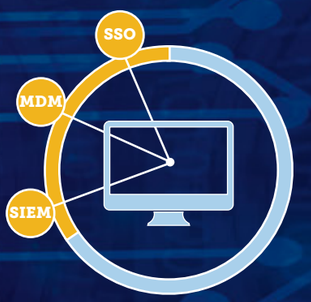
Federführend

In mittleren und großen Unternehmen ist vor allem die IT-Abteilung für IAM verantwortlich; in kleinen Firmen bis zu 100 Mitarbeitern dominiert hingegen die Geschäftsführung.

Partnerwahl

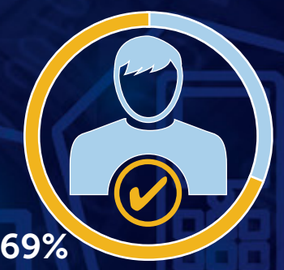
42%

42 Prozent der Unternehmen achten bei der Wahl eines externen (IT-Security-) Dienstleisters auf Firmensitz und Rechenzentrum in Deutschland.



Mangelware

Nur rund ein Drittel der Unternehmen setzt Lösungen für Single-Sign-On (SSO), Mobile Device Management (MDM) oder Security Information und Event Management (SIEM) ein.



Klar definiert

69 Prozent der Unternehmen haben durch die genaue Definition der Rollen der Mitarbeiter bereits die Basis für effizientes IAM geschaffen.

Die Key Findings im Einzelnen

Identity- & Access-Management 2017

1. IT-Security: Die größte Gefahr kommt von außen

Die meisten Firmen sehen die allgemeine Bedrohungslage von extern als größte Herausforderung in Bezug auf IT-Security an.

38 Prozent der Firmen betrachten externe Risiken als größte Herausforderung für ihre IT-Security. Überdurchschnittlich hoch sind die Werte bei kleinen Unternehmen mit weniger als 100 Mitarbeitern (49 Prozent) und bei Firmen mit einem IT-Etat unter einer Million Euro (52 Prozent). Auch fast die Hälfte der Firmen ohne softwaregestütztes IAM (47 Prozent) fürchtet sich vor externen Bedrohungen.

Auch der Faktor Geld spielt eine wichtige Rolle. 27 Prozent der Firmen sehen eine große Herausforderung durch ein zu niedriges (IT-)Security-Budget. Dies gilt insbesondere für große Unternehmen ab 1.000 Mitarbeitern (35 Prozent).

Ein Viertel der Firmen schätzt das Risikopotenzial, das von internen Mitarbeitern ausgeht, sowie fehlende Informationen und mangelnde Transparenz über den Wert bedrohter Daten und Prozesse hoch ein. Neben Compliance-Anforderungen und fehlender Security-Awareness bei den eigenen Mitarbeitern (jeweils 24 Prozent) stellen auch Schatten-IT und Fachkräftemangel (jeweils 23 Prozent) relevante Security-Herausforderungen dar – letztere beide mit 32 und 34 Prozent der Nennungen insbesondere bei großen Unternehmen.

Was sind in Ihren Augen für die Unternehmen die größten Herausforderungen in Bezug auf IT-Security?

Mehrfachnennungen möglich. Angaben in Prozent. Dargestellt sind Nennungen mit über 20 Prozent. Basis: n = 385

	Unternehmen gesamt	Ergebnis-Split nach Anzahl der Mitarbeiter < 100	100 – 999	1.000 +
Allgemeine Bedrohungslage von extern	37,9	49,2	31,1	31,0
Zu niedriges (IT-)Security-Budget	26,5	22,2	25,4	34,5
Risikopotenzial, das von internen Mitarbeitern ausgeht	24,7	21,4	27,0	27,6
Fehlende Informationen über den Wert bedrohter Daten und Prozesse	24,7	27,0	22,2	26,7
Gesetzliche Vorgaben/ Compliance-Anforderungen	24,4	24,6	22,2	29,3
Fehlende Security-Awareness/ fehlendes Training bei eigenen Mitarbeitern	23,6	20,6	23,8	30,2
Schatten-IT	23,4	15,9	23,0	31,9
Fachkräftemangel im Markt	23,1	15,1	21,4	33,6
Echtzeitüberblick über alle Aktivitäten in Systemen, Netzwerken, Datenbanken und Anwendungen	22,1	21,4	18,3	29,3
Personelle Ressourcen im Unternehmen (Anzahl der Mitarbeiterstellen)	20,8	15,9	23,0	26,7
Einbindung von Identity- & Access-Management in Gesamt-Sicherheitsstrategie	20,3	11,9	21,4	30,2

2. EU-Datenschutz-Grundverordnung fordert die Unternehmen

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) tritt am 25. Mai 2018 rechtswirksam in Kraft. Ihre Umsetzung gilt bei den befragten Unternehmen als größte Compliance-Herausforderung.

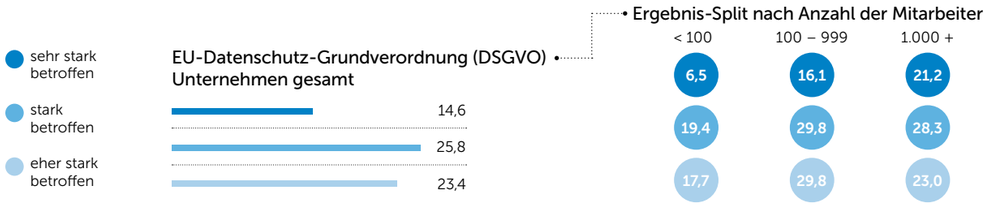
Rund 41 Prozent der Firmen sind von der EU-DSGVO sehr stark (15 Prozent) oder stark betroffen (26 Prozent). Dies gilt vor allem für große Unternehmen ab 1.000 Mitarbeitern beziehungsweise Firmen mit einem IT-Etat ab einer Million Euro (jeweils 50 Prozent). Die kleinen Firmen stehen den Anforderungen der EU-DSGVO gelassener gegenüber. Die Hälfte der kleinen Unternehmen mit weniger als 100 Mitarbeitern sieht sich eher nicht, nicht oder überhaupt nicht betroffen – hoffentlich keine Fehleinschätzung, die die Unternehmen aufgrund der Komplexität der Thematik teuer zu stehen kommen könnte.

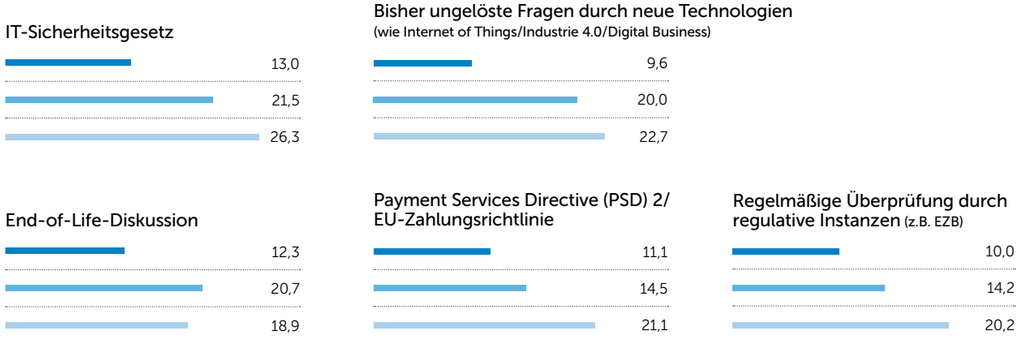
Weitere wichtige Herausforderungen sind das IT-Sicherheitsgesetz (35 Prozent) und die End-of-Life-Diskussion (33 Prozent). Auch hier sind die mittleren und großen Unternehmen jeweils überdurchschnittlich betroffen (44 Prozent).

30 Prozent der Firmen beschäftigen sich zudem verstärkt mit bisher ungelösten Fragen durch neue Technologien (wie Internet of Things / Industrie 4.0 / Digital Business) oder der EU-Zahlungsrichtlinie Payment Services Directive (PSD). Auch diese Punkte betreffen die mittleren und großen Unternehmen stärker als die kleinen Firmen.

Die folgenden Themenfelder stellen Compliance-Herausforderungen dar. In welchem Umfang ist Ihr Unternehmen jeweils betroffen?

Angaben in Prozent. Abfrage auf einer Skala von 1 (sehr stark betroffen) bis 6 (überhaupt nicht betroffen). Dargestellt sind die Top-3-Skalenwerte. Basis: n = 385





3. Nachholbedarf bei softwaregestütztem Identity- & Access-Management

Derzeit setzt nur etwas mehr als ein Drittel der befragten Firmen eine Softwarelösung für Identity- & Access-Management (IAM) ein. Vorreiter sind die großen Unternehmen.

38 Prozent der befragten Unternehmen nutzen ein softwaregestütztes IAM. Immerhin 31 Prozent der Firmen planen den Einsatz einer IAM-Software, für 28 Prozent kommt die Einführung derzeit nicht infrage.

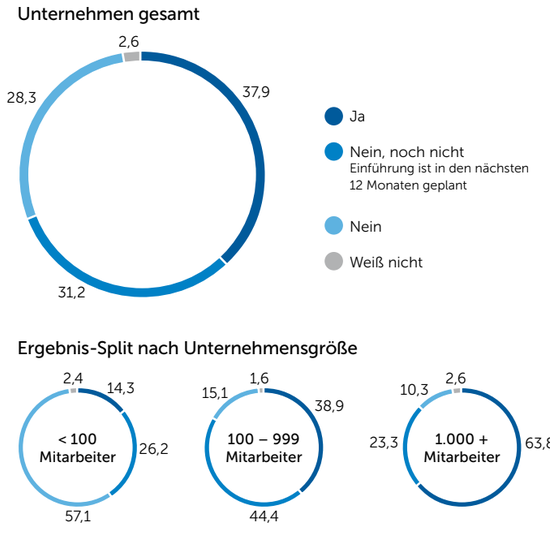
Interessant ist ein Blick auf die unterschiedliche Bewertung in den Fachbereichen der Unternehmen. Während die Hälfte der CIOs und der IT-Leiter den Einsatz einer IAM-Lösung bejahen, sind es bei den Geschäftsführern nur 22 Prozent.

Vorreiter bei softwaregestütztem IAM sind die großen Unternehmen mit einem Wert von 64 Prozent, gefolgt von den mittleren Firmen mit 39 Prozent. Nur 14 Prozent der kleinen Unternehmen nutzen eine IAM-Software. Entsprechend planen derzeit auch 57 Prozent der Firmen mit bis zu 100 Mitarbeitern noch nicht den Einsatz einer entsprechenden Lösung.

In Firmen mit installierter IAM-Software greifen vor allem die Mitarbeiter intern (75 Prozent) oder extern (60 Prozent) über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme ihres Unternehmens zu. In 42 Prozent der Firmen erhalten Geschäftspartner, Dienstleister und Zulieferer (B2B) über IAM Zugang zum Netzwerk, in 23 Prozent die Kunden sowie auch Dienste und Services über Machine-to-Machine-Kommunikation (M2M).

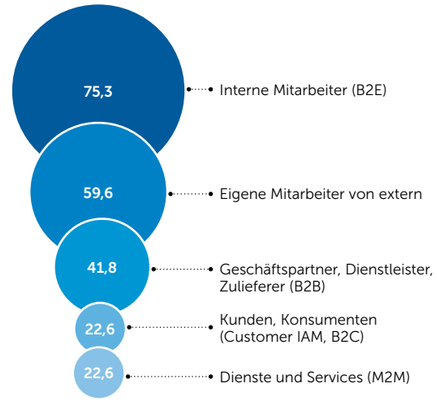
Gibt es in Ihrem Unternehmen ein softwaregestütztes Identity- & Access-Management?

Angaben in Prozent. Basis: n = 385



Wer (oder was) greift über Authentifizierungs-und Identitätsmanagement-Tools auf Systeme Ihres Unternehmens zu?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 146 (Filter: Nur Unternehmen mit softwaregestütztem Identity- und Access-Management)



4. Mut zur Lücke: Multi-Faktor-Authentifizierung noch nicht komplett umgesetzt

Etwas mehr als ein Fünftel der Firmen sichert ihre Zugänge zum Netzwerk NICHT über eine Multi-Faktor-Authentifizierung mit Token (Hardware, Software oder Push) ab.

Insgesamt 21 Prozent der Unternehmen setzen derzeit nicht auf die Multi-Faktor-Authentifizierung; zumindest die Hälfte davon (elf Prozent) plant aber bereits die Implementierung. Überdurchschnittlich hoch ist hier der Anteil kleiner Unternehmen.

69 Prozent der befragten Firmen nutzen die Multi-Faktor-Authentifizierung (MFA) für die eigenen Mitarbeiter. Das gilt vor allem für Unternehmen mittlerer Größe zwischen 100 und 999 Mitarbeitern (76 Prozent).

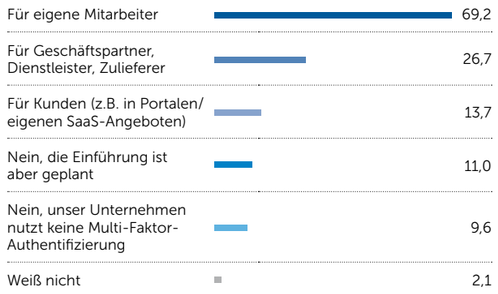
In 27 Prozent der Unternehmen müssen sich Geschäftspartner, Dienstleister und Zulieferer auf mehreren Wegen authentifizieren. Nur 6 Prozent der kleinen Unternehmen haben dies auf ihrer Agenda.

Für ihre Kunden in Portalen oder eigenen Cloud-Anwendungen (SaaS) setzen 14 Prozent der Firmen auf die Multi-Faktor-Authentifizierung. Hier tun sich vor allem die großen Unternehmen hervor (20 Prozent).

Smartphone (45 Prozent) und Smartcard (44 Prozent) werden am häufigsten für die Multi-Faktor-Authentisierung genutzt, gefolgt von USB (37 Prozent), SIM-Karte (30 Prozent), Biometrie (23 Prozent) und MicroSD (18 Prozent).

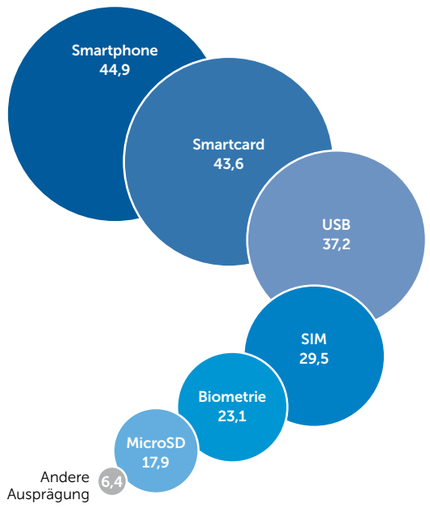
Nutzt Ihr Unternehmen für die Absicherung der Zugänge eine Multi-Faktor-Authentifizierung mit Token (Hardware, Software oder Push)?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 146 (Filter: Nur Unternehmen mit softwaregestütztem Identity- & Access-Management)



Welche Ausprägungen einer Multi-Faktor-Authentisierung finden beim SSO in Ihrem Unternehmen Anwendung?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 78 (Filter: Nur Unternehmen mit Single-Sign-On (SSO) nur als Multi-Faktor-Authentisierung)



5. Die IT-Abteilung gibt bei IAM meistens den Ton an

In mittleren und großen Unternehmen ist vor allem die IT-Abteilung für IAM verantwortlich, in kleinen Firmen bis zu 100 Mitarbeitern hingegen die Geschäftsführung.

In etwas mehr als einem Drittel (35 Prozent) der befragten Unternehmen ist die Geschäftsführung für das Identity- & Access-Management verantwortlich.

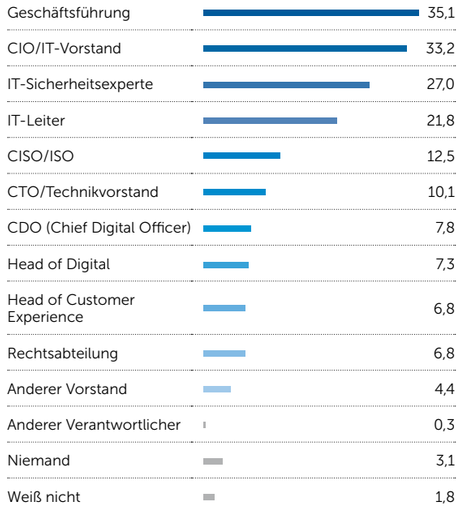
Die Werte sind auch von der Größe des Unternehmens abhängig. Während sich in 62 Prozent der kleinen Firmen der Geschäftsführer um IAM kümmert, sind es in mittleren Firmen nur 18 Prozent, in großen Unternehmen 28 Prozent.

Insgesamt haben beim Thema IAM erwartungsgemäß die IT-Experten den Hut auf. Die hohe Zahl der Nennungen ist zudem ein Indiz dafür, dass es nicht nur einen Verantwortlichen gibt, sondern im Team entschieden wird. Das gilt insbesondere für mittlere und große Unternehmen, was aufgrund der zunehmenden Komplexität der Strukturen leicht nachvollziehbar ist.

Ein ähnliches Bild ergeben die Antworten auf die Frage, wer in den Firmen die Entscheidungen bei der Auswahl von Security-Dienstleistern und Security-Lösungen trifft. Auch hier dominieren in kleinen Firmen die Geschäftsführer (75 Prozent), in den mittleren und großen Unternehmen der CIO oder IT-Leiter. Und auch hier deutet die hohe Anzahl an Mehrfachnennungen darauf hin, dass diese Entscheidungen im Team getroffen werden.

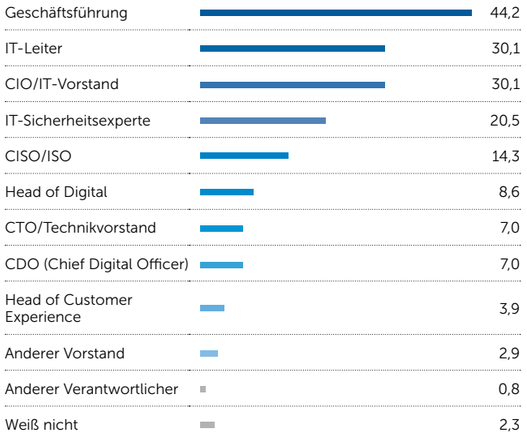
Wer in Ihrem Unternehmen ist für das Identity- & Access-Management verantwortlich?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 385



Wer in Ihrem Unternehmen trifft die Entscheidungen bezüglich der Auswahl von Security-Dienstleistern und Security-Lösungen?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 385



6. Externe IAM-Dienstleister sind gefragt

Die Mehrheit der Unternehmen arbeitet beim Thema IAM mit einem oder mehreren externen Partnern zusammen. Das Gros der kleinen Firmen hingegen setzt auf eigenes Know-how.

59 Prozent der Unternehmen holen sich für das Identity- & Access-Management einen (42 Prozent) oder sogar mehrere Dienstleister (17 Prozent) ins Boot.

Auffällig sind hier die hohen Werte bei mittleren und großen Unternehmen mit insgesamt 71 Prozent (mittel) beziehungsweise 78 Prozent (groß), während nur 28 Prozent der kleinen Firmen mit einem oder mehreren Dienstleistern zusammenarbeiten.

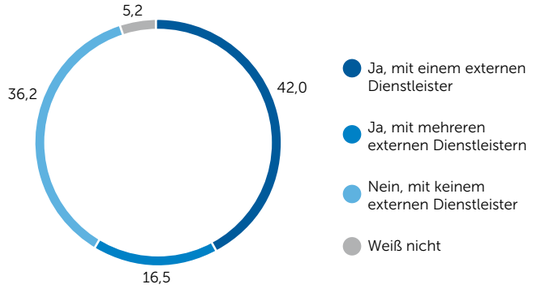
Entsprechend setzen zwei Drittel (66 Prozent) der Unternehmen mit bis zu 100 Mitarbeitern IAM selbst ohne externe Hilfe um. Analog gilt das auch für Firmen mit einem kleineren IT-Etat unter einer Million Euro (59 Prozent).

Die meisten Firmen zögern aber (noch) mit einer kompletten Auslagerung ihres IAMs. So greifen derzeit nur 17 Prozent der Befragten auf die Dienste eines Identity-Providers zurück, 16 Prozent planen diese Aktion.

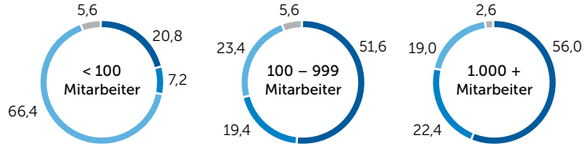
Arbeitet Ihr Unternehmen im Bereich Identity- und Access-Management mit einem oder mehreren externen Dienstleistern zusammen?

Angaben in Prozent. Basis: n = 381

Unternehmen gesamt

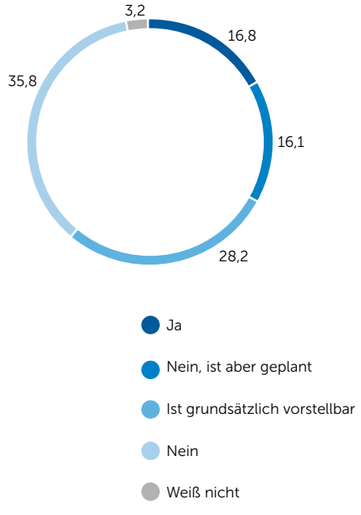


Ergebnis-Split nach Unternehmensgröße



Greift Ihr Unternehmen auf die Dienste eines Identity-Providers zurück? Ist Ihr IAM komplett ausgelagert?

Angaben in Prozent. Basis: n = 380



7. Firmensitz, Sicherheit, Qualität und Preis sind die Argumente bei der Auswahl eines externen Anbieters

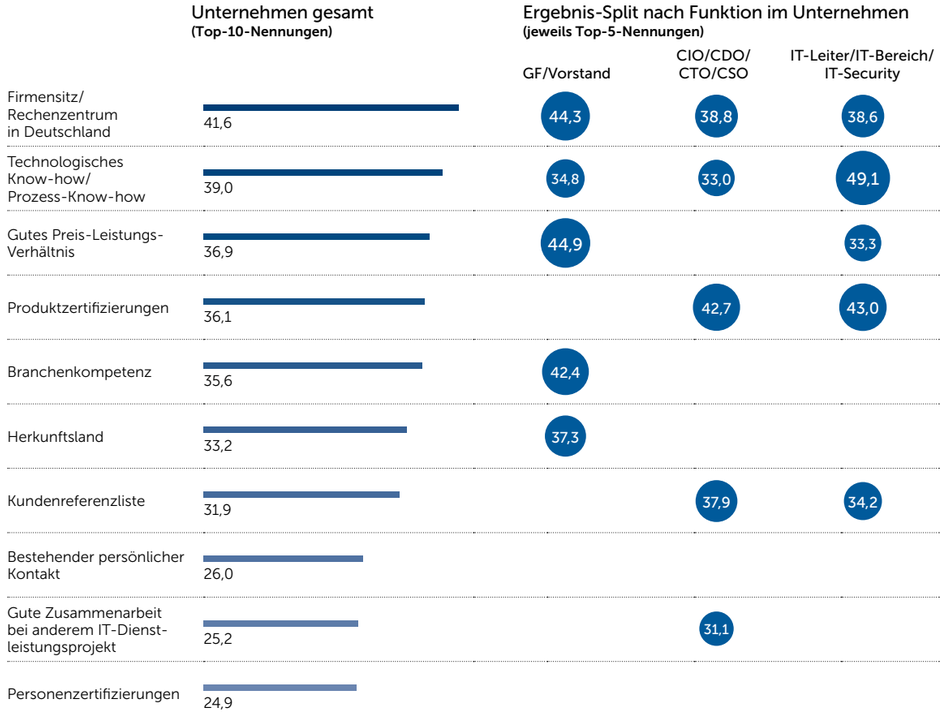
Unternehmen legen bei der Wahl eines externen Partners vor allem Wert auf ein Rechenzentrum in Deutschland, Technologieexpertise sowie ein gutes Preis-Leistungs-Verhältnis.

Über alle Unternehmen und Funktionsbereiche hinweg sind fünf Kriterien in etwa gleich wichtig bei der Auswahl eines externen IT-Security-Dienstleisters: Mit 42 Prozent wird als wichtigstes Auswahlkriterium „Firmensitz/Rechenzentrum in Deutschland" genannt, gefolgt von technologischem und Prozess-Know-how (39 Prozent) und dahinter mit 37 Prozent einem guten Preis-Leistungs-Verhältnis. Produktzertifizierungen und Branchenkompetenz kommen jeweils auf 36 Prozent.

Ein etwas anderes Bild ergibt sich bei einem Blick auf die Antworten nach Funktionen im Unternehmen. Schnell erkennt man, wer welche Prioritäten setzt: Während Geschäftsführer gerne nach dem besten Preis Ausschau halten, wird auf der Arbeitsebene mehr auf fachliche und qualitative Aspekte geachtet.

Was sind für Sie entscheidende Kriterien bei der Auswahl eines externen (IT-Security-)Dienstleisters?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 385



8. Das Passwort ist und bleibt die wichtigste Methode der Authentifizierung

Das Passwort ist heute und nach Einschätzung der Firmen auch in fünf Jahren noch die wichtigste Methode der Authentifizierung – deutlich an Relevanz gewinnen aber biometrische Methoden und APPs.

In 62 Prozent der Unternehmen ist das Passwort heute die wichtigste Methode zur Authentifizierung, in fünf Jahren soll das Passwort in 53 Prozent der Firmen zum Einsatz kommen. Damit ist und bleibt das Passwort mit Abstand die wichtigste Methode im Rahmen der Multi-Faktor-Authentifizierung.

Den zweiten Platz nimmt die PIN ein mit 39 Prozent (jetzt) und 40 Prozent (in fünf Jahren).

Aktuell liegt die E-Mail mit 35 Prozent auf dem Bronze-Platz; in fünf Jahren (34 Prozent) wird sie jedoch vom Fingerabdruck auf den vierten Platz verdrängt. Die Bedeutung des Fingerabdrucks steigt von jetzt 19 Prozent (aktuell Platz sechs) auf 37 Prozent in fünf Jahren.

Ebenso gewinnen biometrische Merkmale wie Gesichtserkennung, Stimmerkennung sowie Iriserkennung oder Retinamerkmale (Augenhintergrund) als Authentifizierungsmethoden deutlich an Bedeutung. Ebenfalls einen großen Bedeutungszuwachs (plus 13 Prozentpunkte) erlangen die heute nur zu elf Prozent genutzten Smartphone-Apps.

Welche Methoden zur Authentifizierung von Nutzern kommen in Ihrem Unternehmen schon heute zum Einsatz und werden in fünf Jahren in Ihrem Unternehmen zum Einsatz kommen?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 385

bereits im Einsatz		Einsatz in fünf Jahren	Veränderung in %-Punkten
61,6	Passwort	52,7	- 8,9
39,2	PIN	40,3	+ 1,1
35,3	E-Mail	34,0	- 1,3
28,3	Sicherheitsfrage	31,9	+ 3,6
21,6	Chip-/Magnetstreifenkarte/RFID-Karte	28,3	+ 6,7
18,7	Fingerabdruck	36,9	**+ 18,2**
11,9	Gesichtserkennung	27,3	**+ 15,4**
11,2	TAN- und iTAN-Liste	14,8	+ 3,6
10,9	Smartphone App	24,2	**+ 13,3**
10,4	SIM-Karte	15,1	+ 4,7
10,1	Handschrift (Unterschrift)	13,2	+ 3,1
10,1	Iriserkennung/Retinamerkmale (Augenhintergrund)	18,2	**+ 8,1**
8,8	One Time PIN Token	12,5	+ 3,7
8,6	Stimmerkennung	19,2	**+ 10,6**
7,8	Anruf	7,3	- 0,5
6,0	Erbinformation (DNS)	6,5	+ 0,5
5,7	(neuer) Personalausweis	11,7	+ 6,0
5,2	Handlinienstruktur/Handgeometrie (Handflächenscanner)	8,3	+ 3,1
1,0	Federationansatz – Nutzung vertrauenswürdiger externer IDs	2,6	+ 1,6

9. Lösungen für SSO, MDM und SIEM sind in Unternehmen Mangelware

Nur rund ein Drittel der Unternehmen setzt jeweils Lösungen für Single-Sign-On (SSO), Mobile Device Management (MDM) oder Security Information und Event Management (SIEM) ein.

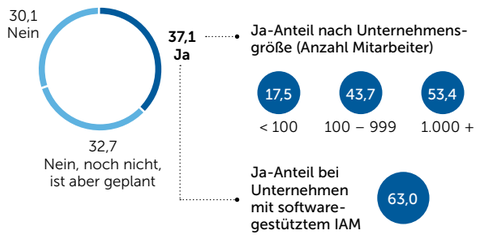
Nur 37 Prozent der befragten Firmen setzen eine SSO-Lösung für die einfachere Anmeldung bei ihren Systemen ein. Die Nase vorn haben hier die großen Firmen mit 53 Prozent, während nur 18 Prozent der kleinen Unternehmen SSO nutzen. Absolute SSO-Vorreiter mit 63 Prozent sind hier die Unternehmen, die bereits ein softwaregestütztes IAM installiert haben.

Ein ähnliches Bild ergibt sich bei den MDM-Lösungen für die sichere und zentrale Verwaltung von mobilen Geräten wie Smartphones und Tablets. Während in der Gesamtheit nur 37 Prozent der Unternehmen auf MDM setzen, sind es bei den Firmen mit installiertem IAM 61 Prozent. Auch bei MDM steigt der Reifegrad mit der Unternehmensgröße an. Nur 14 Prozent der kleineren Firmen besitzen eine MDM-Lösung; der Wert klettert bei den Unternehmen mittlerer Größe auf 44 Prozent bis hin zu 53 Prozent bei den großen Firmen ab 1.000 Mitarbeitern.

Wenig überraschend ist dies auch bei SIEM-Lösungen der Fall, also beim softwaregestützten Sicherheitsinformations- und Ereignismanagement in Echtzeit. Im Schnitt setzen 30 Prozent der Firmen eine SIEM-Lösung ein. Allerdings tun dies nur 14 Prozent der kleinen Unternehmen. Die mittleren und großen Firmen liegen mit 37 und 40 Prozent deutlich über dem Schnitt. Auch hier stehen die Firmen mit softwaregestütztem IAM an der Spitze (60 Prozent).

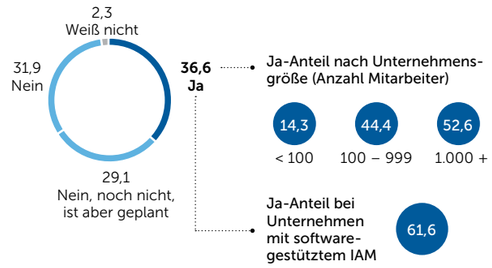
Gibt es für die Mitarbeiter Ihres Unternehmens eine Single-Sign-On (SSO)-Lösung?

Angaben in Prozent. Basis: n = 385



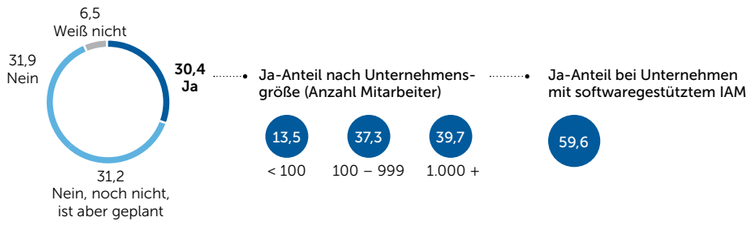
Setzt Ihr Unternehmen eine MDM-Lösung ein (Mobile Device Management)?

Angaben in Prozent. Basis: n = 385



Gibt es in Ihrem Unternehmen eine SIEM-Lösung, also ein softwaregestütztes Sicherheitsinformations- und Ereignismanagement in Echtzeit?

Angaben in Prozent. Basis: n = 385



10. Rollen der Mitarbeiter sind definiert, Basis für effizientes IAM geschaffen

69 Prozent der Unternehmen haben die Rolle eines jeden Mitarbeiters so genau definiert, dass sich daraus alle Zugänge oder Zugriffsberechtigungen für IAM eindeutig ableiten lassen.

Interessant ist hier ein Blick auf die Unternehmensgrößen. Hier sind die Unterschiede im Vergleich zu anderen Themen relativ gering: Immerhin 63 Prozent der kleinen Firmen haben die Rollen der einzelnen Mitarbeiter genau definiert, bei den mittleren sind es 74 Prozent, bei den großen Unternehmen 73 Prozent.

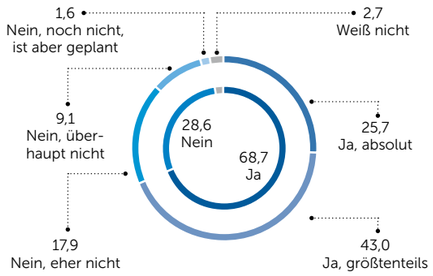
Vorreiter sind logischerweise die Firmen mit softwaregestütztem IAM (82 Prozent).

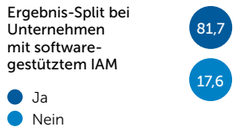
29 Prozent der Unternehmen müssen die Rollen ihrer Mitarbeiter noch genau definieren, um alle Zugriffsberechtigungen eindeutig ableiten zu können.

Die rollenbasierte Administration (Role-based Access Control, RBAC) stellt grundsätzlich das wichtigste Administrationskonzept im IAM von Unternehmen dar. 56 Prozent der Firmen setzen auf diesen modernen Ansatz.

Ist in Ihrem Unternehmen die Rolle eines jeden Mitarbeiters so genau definiert, dass sich daraus alle Zugänge oder Zugriffsberechtigungen eindeutig ableiten lassen?

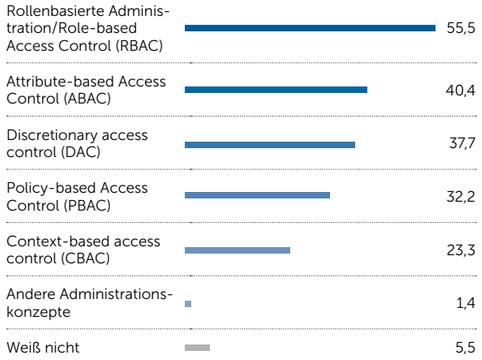
Angaben in Prozent. Basis: n = 374





Welche Administrationskonzepte nutzten Sie in Ihrem IAM?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 146 (Filter: Nur Unternehmen mit softwaregestütztem Identity- & Access-Management)



Die Studienergebnisse im Einzelnen

1. Zukunft: Cyber-Angriffe als Bedrohung Nummer eins

Die befragten Firmen sehen zahlreiche Bedrohungsszenarien durch digitale Kriminalität – je nach Unternehmensbereich aber unterschiedlich.

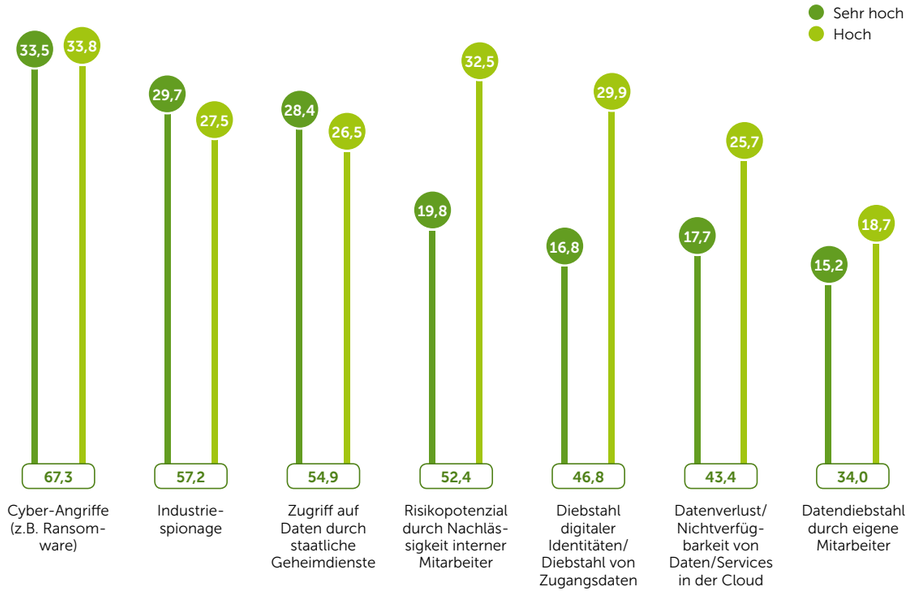
67 Prozent der Unternehmen schätzen für die Zukunft die Bedrohung durch Cyber-Angriffe sehr hoch oder hoch ein. Dies gilt vor allem für große Unternehmen ab 1.000 Mitarbeitern (72 Prozent).

Mit etwas Abstand folgen Datendiebstahl durch den Wettbewerb in Form von Industriespionage (57 Prozent) und der Zugriff auf Daten durch staatliche Geheimdienste (55 Prozent). Überdurchschnittlich besorgt sind hier jeweils die Technologieentscheider; mit 60 beziehungsweise 62 Prozent schätzen sie diese beiden Gefahren deutlich höher ein als die Geschäftsführer und IT-ler.

Nicht unerheblich ist auch die Sorge vor den Fehlern beziehungsweise krimineller Energie der eigenen Mitarbeiter. 52 Prozent fürchten Risiken durch Nachlässigkeiten der Mitarbeiter, wobei hier die CIOs/CDOs/CTOs mit 61 Prozent besonders kritisch sind. Im Schnitt misstraut ein gutes Drittel aller Unternehmen ihren Mitarbeitern (34 Prozent befürchten Datendiebstahl durch sie) – auch hier „führen" die Technologieentscheider mit 41 Prozent.

Hier sind nun einige Bedrohungsszenarien skizziert. Wie hoch schätzen Sie das künftige Ausmaß der Bedrohung jeweils ein?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 385
Dargestellt sind Bedrohungsarten, die als „sehr hoch" bzw. „hoch" eingestuft wurden.



2. Ausbaufähig: Strategien für Digitalisierung, IT-Security und Risikobewertung

Nicht alle Firmen verfügen über Strategien im digitalen Bereich, und noch weniger sind sich alle in den Unternehmen einig darüber, ob und welche Strategien es überhaupt gibt.

In 65 Prozent der befragten Firmen gibt es eine Digitalisierungsstrategie. Wenig überraschend sind hier die hohen Werte bei mittleren und großen Unternehmen mit 77 und 78 Prozent und die eher geringen bei kleinen Firmen (42 Prozent).

Interessant ist der Blick auf die Angaben nach Funktionen im Unternehmen. Die Technologieentscheider scheinen mehr zu wissen als ihre Chefs, denn immerhin 77 Prozent (im Vergleich zu 55 Prozent der Geschäftsführer) sagen, dass es eine Digitalisierungsstrategie gibt. Oder schlummern in ihren Schubladen Konzepte, die nur noch nicht hinreichend kommuniziert wurden? Diese unterschiedliche Einschätzung zieht sich durch alle Strategiebereiche, am deutlichsten bei der Frage nach der IT-Security-Strategie.

71 Prozent der Firmen verfolgen bei ihren Sicherheitsmaßnahmen einen ganzheitlichen Plan, nach Ansicht der Geschäftsführer jedoch nur 59 Prozent, nach Ansicht der CIOs/CDOs und CTOs starke 87 Prozent.

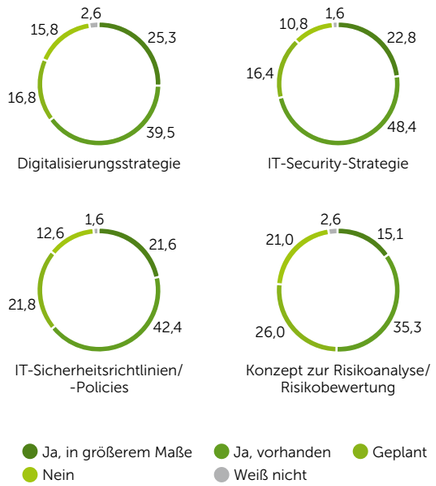
Einigkeit herrscht bei der Frage, ob die IT-Security- und die Digitalisierungsstrategie miteinander verknüpft sind. Bei 82 Prozent ist dies der Fall, und das wissen auch alle.

Ausbaufähig sind in den Unternehmen zudem die IT-Sicherheitsrichtlinien/-Policies (64 Prozent) sowie die Konzepte zur Risikoanalyse und Risikobewertung (50 Prozent).

Welche der folgenden Strategien und Konzepte gibt es in Ihrem Unternehmen?

Angaben in Prozent. Basis: n = 385

Unternehmen gesamt



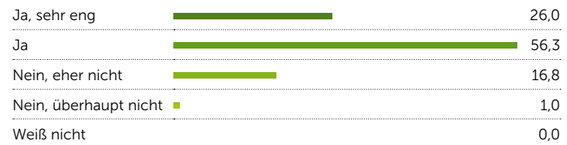
Ergebnis-Split nach Funktion im Unternehmen

(„Ja, in größerem Maße" und „Ja, vorhanden")

	Gesamt	GF/ Vorstand	CIO/CDO/ CTO/CSO	IT-Leiter/IT-Bereich/ IT-Security
Digitalisierungsstrategie	64,8	55,4	76,8	67,6
IT-Security-Strategie	71,2	59,1	87,0	75,4
IT-Sicherheitsrichtlinien/ -Policies	64,0	51,9	70,0	74,6
Konzept zur Risikoanalyse/Risikobewertung	50,4	37,9	60,2	59,6

Sind in Ihrem Unternehmen IT-Security- und Digitalisierungsstrategie miteinander verknüpft?

Angaben in Prozent. Basis: n = 208. (Filter: Nur Unternehmen, die gleichzeitig über eine Digitalisierungs- und eine IT-Security-Strategie verfügen)



3. Große Unternehmen sind bei IAM am besten aufgestellt

Beim IAM-Reifegrad stufen sich die Firmen auf einer Skala von 0 (Wir stehen am Anfang) bis 10 (Zukunftssicheres IAM) im Mittelfeld ein. Pioniere sind die großen Unternehmen.

Mit einem arithmetischen Mittel von 5,95 ist beim Reifegrad in Bezug auf Identity- & Access-Management noch Luft nach oben.

Die großen Unternehmen (arithmetisches Mittel 6,63) sind beim Thema IAM weiter als die mittleren (6,31) und kleinen (5,03) Firmen.

Naturgemäß am höchsten ist der Wert bei Unternehmen mit softwaregestütztem IAM (7,14), während die Firmen ohne softwaregestütztes IAM hier ein arithmetisches Mittel von 4,67 erreichen.

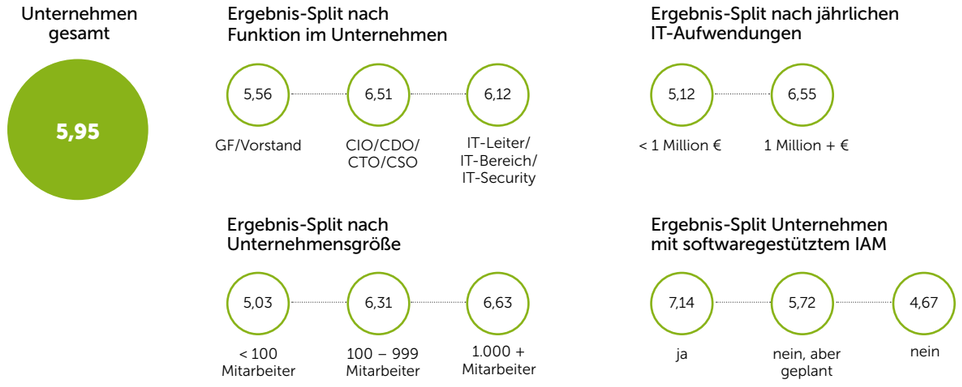
Nur fünf Prozent der befragten Unternehmen verfügen ihrer Meinung nach über ein absolut zukunftssicheres IAM (= Wert 10 auf der Skala), bei den großen Unternehmen sind es zehn Prozent.

Das Gros der Firmen (53 Prozent) bewegt sich auf der Skala im oberen Mittelfeld zwischen 5 und 7.

Beruhigend: Nur zwei Prozent der Unternehmen stehen bei IAM ganz am Anfang.

Wie würden Sie den Reifegrad Ihres Unternehmens in Bezug auf sein Identity- & Access-Management einstufen?

Mittelwertangaben. Abfrage auf einer Skala von 0 (= Unser Unternehmen steht hier noch ganz am Anfang) bis 10 (= Unser Unternehmen verfügt über ein zukunftssicheres IAM). Basis: n = 382



4. IAM ist Top-Thema bei Zusammenarbeit mit IT-Security-Dienstleistern

Drei Viertel der Unternehmen arbeiten mit externen IT-Security-Dienstleistern zusammen. Wichtigstes Gebiet ist das Identity- & Access-Management.

77 Prozent der befragten Unternehmen arbeiten beim Thema Security mit externen Dienstleistern zusammen. Ein knappes Viertel verzichtet vollständig darauf, wobei der Wert vor allem bei den kleinen Firmen auf 50 Prozent steigt. Bei den mittleren und großen Unternehmen sichern nur neun beziehungsweise zehn Prozent ihre IT-Infrastruktur ohne Unterstützung von außen ab.

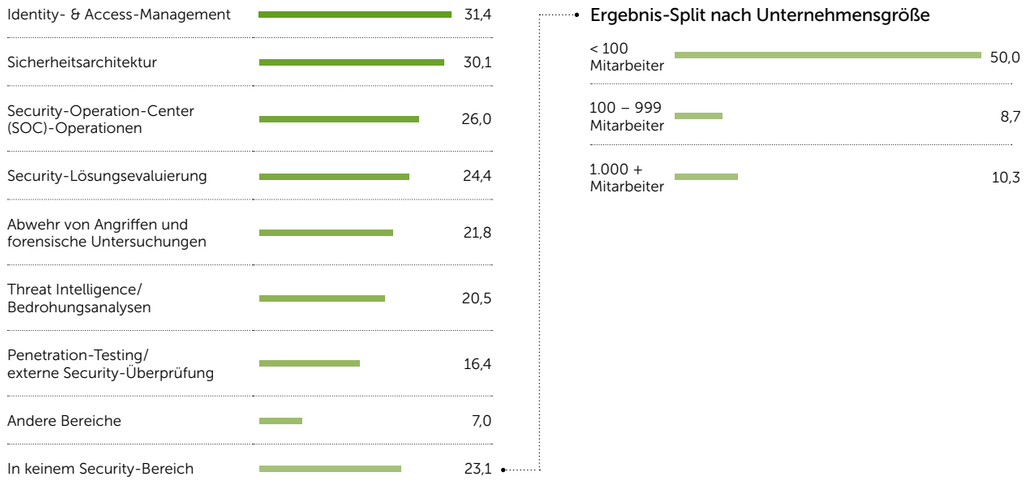
Wichtigstes Gebiet bei der Zusammenarbeit mit den Dienstleistern ist das Identity- & Access-Management (31 Prozent), gefolgt von der Sicherheitsarchitektur (30 Prozent) und dem Betrieb eines Security Operation Centers (SOC, 26 Prozent).

Letzteres ist vor allem in mittleren (36 Prozent) und großen Firmen (35 Prozent) der Fall. Nur sieben Prozent der kleinen Unternehmen setzen beim Thema SOC auf einen externen Partner.

Weitere Gebiete für die Zusammenarbeit mit externen IT-Security-Dienstleistern sind die Evaluation von Security-Lösungen (24 Prozent), die Abwehr von Angriffen und forensische Untersuchungen (22 Prozent), Threat Intelligence mit Bedrohungsanalysen (21 Prozent) und Penetrationstests (16 Prozent).

Auf welchen Gebieten arbeitet Ihr Unternehmen mit externen Dienstleistern zusammen?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 385



5. Bei der Umsetzung der EU-DSGVO besteht noch Handlungsbedarf

Das Gros der Firmen sieht sich auch dank eines zentralen Ansprechpartners gut auf die EU-DSGVO vorbereitet. Nichtsdestotrotz besteht noch Handlungsbedarf.

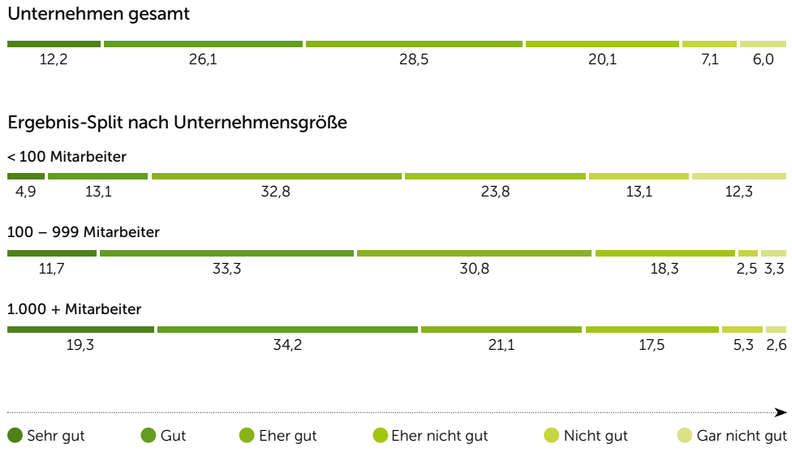
Vier von zehn Firmen sagen, dass sie gut bis sehr gut auf die Herausforderungen vorbereitet sind, die die Europäische Datenschutz-Grundverordnung mit sich bringt. Mittlere und große Unternehmen (45 und 54 Prozent) sind halbwegs gerüstet, während bei kleinen Firmen (18 Prozent) noch größerer Nachholbedarf besteht.

Nichtsdestotrotz sehen 66 Prozent der Firmen noch sehr großen bis eher großen Handlungsbedarf bis zum Stichtag der EU-DSGVO am 25. Mai 2018. Dass sich die großen Unternehmen viel besser vorbereitet fühlen als die kleinen, trotzdem aber mehr Handlungsbedarf als diese sehen, ist nur auf den ersten Blick ein Paradoxon. Wenn man bedenkt, dass große Firmen vielfältiger betroffen sind und es nach wie vor große Unsicherheiten im Hinblick auf Richtliniendetails gibt, die eine Einschätzung juristischer Konsequenzen erschweren, erscheinen die Ergebnisse doch absolut plausibel.

Um die Anpassung der internen Prozesse an die Anforderungen der EU-DSGVO kümmert sich in 71 Prozent der Unternehmen ein zentraler Ansprechpartner. In den kleinen Firmen ist dies meist der Geschäftsführer (41 Prozent; Durchschnitt 28 Prozent), in den mittleren (44 Prozent) und großen Firmen (43 Prozent) überwiegend die IT-Abteilung (Durchschnitt 35 Prozent). 27 Prozent der Unternehmen haben bisher noch keinen zentralen Ansprechpartner – wobei der Wert bei den kleinen Unternehmen mit 39 Prozent überdurchschnittlich hoch ist.

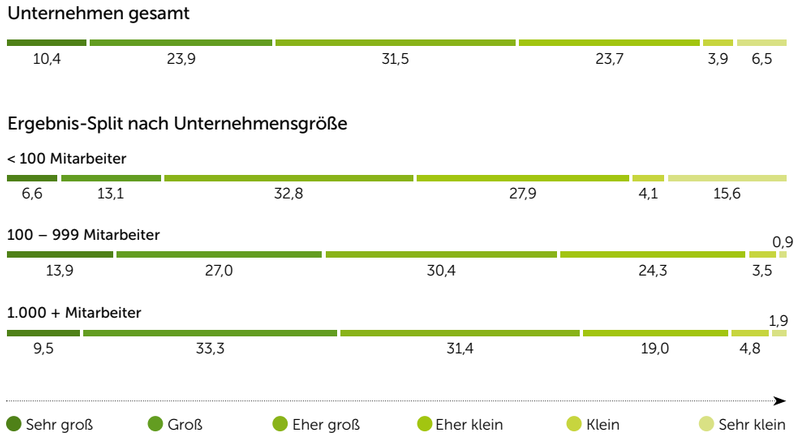
Wie gut sehen Sie Ihr Unternehmen heute auf die Herausforderungen vorbereitet, die die Europäische Datenschutz-Grundverordnung mit sich bringt?

Angaben in Prozent. Abfrage auf einer Skala von 1 (= sehr gut) bis 6 (= gar nicht gut). Basis: n = 368



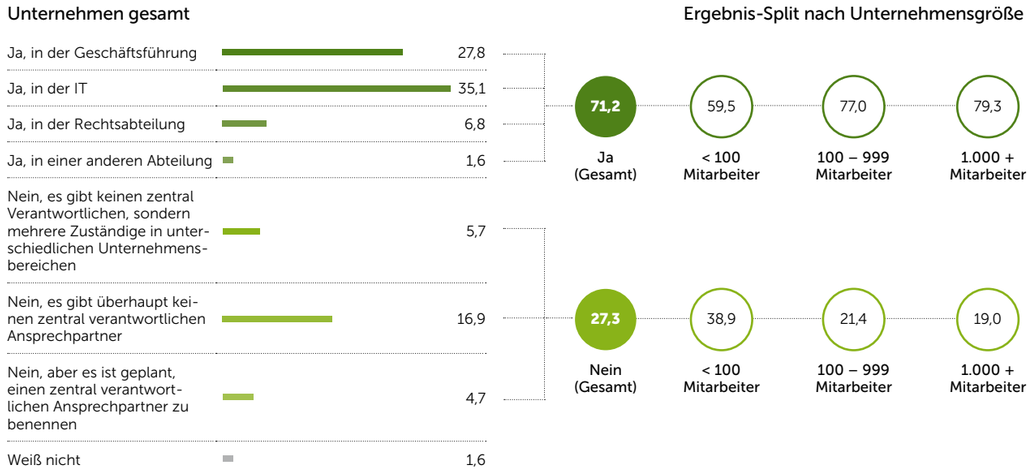
Wie groß schätzen Sie den Handlungsbedarf ein, der durch die EU-Datenschutz-Grundverordnung noch für Ihr Unternehmen erwächst?

Angaben in Prozent. Abfrage auf einer Skala von 1 (= sehr groß) bis 6 (= sehr klein). Basis: n = 355



Gibt es in Ihrem Unternehmen einen zentralen Ansprechpartner, der für die Anpassung der internen Prozesse an die Anforderungen der Europäischen Datenschutz-Grundverordnung verantwortlich ist?

Angaben in Prozent. Basis: n = 385



6. Authentifizierungslösung: Sicherheit ist das wichtigste Kaufkriterium

Sicherheit, Bedienerfreundlichkeit und Produktzertifizierung sind die drei wichtigsten Kriterien, nach denen Unternehmen ihre (Multi-Faktor-)Authentifizierungslösung auswählen – ja nach Unternehmensbereich allerdings mit deutlich anderer Gewichtung.

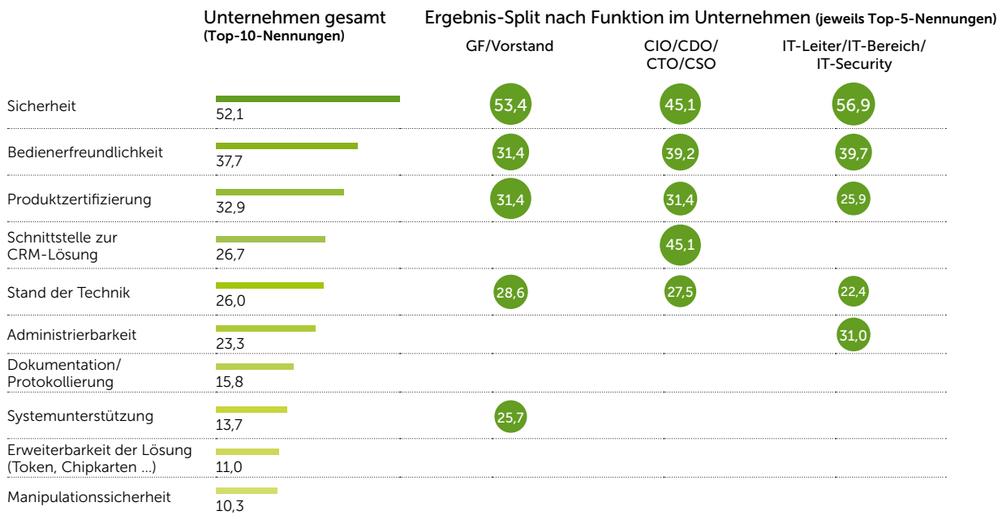
In 52 Prozent der Unternehmen bildet Sicherheit das wichtigste Kriterium für die Auswahl einer (Multi-Faktor-)Authentifizierungslösung, um ihre digitalen Geschäftsprozesse abzusichern. Das ist auch über alle Unternehmensgrößen und -bereiche der Fall, teilweise allerdings mit unterschiedlichen Ausprägungen. So wird die Sicherheit zum Beispiel bei den mittelgroßen Unternehmen mit 100 – 999 Mitarbeitern mit 59 Prozent und von IT-Leitern mit 57 Prozent noch einmal signifikant höher bewertet.

Allerdings schwindet diese Einigkeit in der Bewertung der Wichtigkeit bei allen anderen Kaufkriterien. Hier machen sich die unterschiedlichen Blickwinkel der Hierarchieebenen wieder deutlich bemerkbar.

Bei den technischen Entscheidern steht mit 45 Prozent die Schnittstelle zur CRM-Lösung an zweiter Stelle – ein Kriterium, das Geschäftsführer mit elf Prozent als kaum relevant betrachten. Auch die Bedienerfreundlichkeit wird von den CIOs/CDOs/CTOs mit 39 (IT-ler 40 Prozent) deutlich höher eingestuft als von der Unternehmensführung. Umgekehrt setzt diese das Thema Produktzertifizierung mit 49 Prozent auf Rang zwei, während das bei den anderen eher nachrangig ist. So bleibt auf einen regen und konstruktiven Austausch zwischen den Unternehmensbereichen zu hoffen, bevor neue Systeme final ausgewählt werden.

Was sind für Sie die wichtigsten drei Kriterien zur Auswahl einer (Multi-Faktor-) Authentifizierungslösung, mit deren Hilfe Sie digitale Geschäftsprozesse absichern möchten?

Maximal drei Antwortmöglichkeiten. Top-10-Nennungen (von insgesamt 13 gestützt abgefragten Items). Basis: n = 146 (Filter: Nur Unternehmen mit softwaregestütztem Identity- & Access-Management)



7. Authentifizierung: modulare Lösung bevorzugt

Knapp die Hälfte der Firmen empfiehlt bei der Authentifizierung von Systemen modulare Lösungen. Integrierte Lösungen bilden ihrer Ansicht nach die zweite Wahl.

Insgesamt die Hälfte der Befragten würde anderen Unternehmen bei der Authentifizierung eindeutig (22 Prozent) oder eher (27 Prozent) zu modularen statt zu integrierten Lösungen raten – überdurchschnittlich hoch ist dieser Wert mit 62 Prozent bei den IT-Entscheidern.

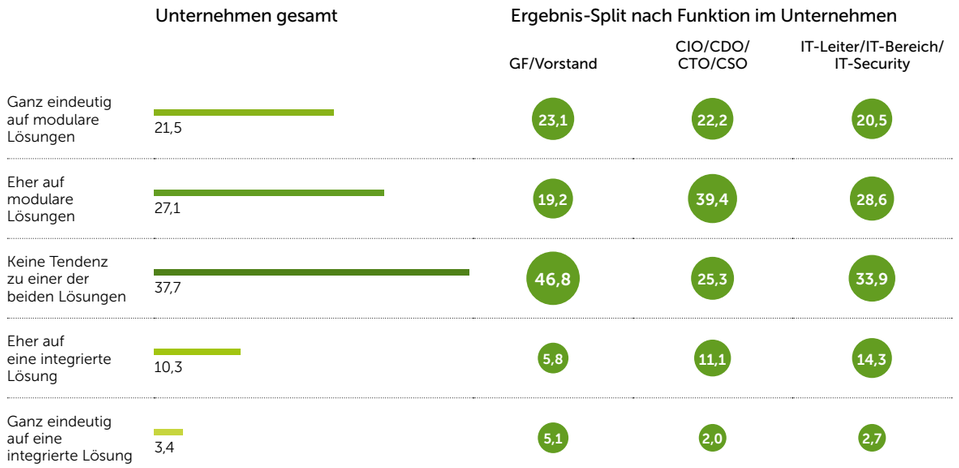
Auch die Firmen, die bereits über ein softwaregestütztes IAM verfügen (62 Prozent), plädieren für den Einsatz einer modularen Lösung.

38 Prozent der Unternehmen sind eher unentschlossen. Hier gibt es keine Tendenz zu einer der beiden Lösungen. Hierzu zählen vor allem kleine Unternehmen mit einem überproportionalen Anteil von 53 Prozent beziehungsweise auch die Geschäftsführer/Vorstände mit 47 Prozent.

Die Zahl der klaren Befürworter einer integrierten Lösung für die Authentifizierung ist sehr gering. Nur knapp 14 Prozent der Firmen raten eher oder ganz eindeutig zu einer integrierten Lösung.

Würden Sie anderen Unternehmen raten, bei der Authentifizierung prinzipiell eher auf modulare oder eher auf integrierte Lösungen zu setzen?

Angaben in Prozent. Basis: n = 377



8. Firmen halten sich bei Self-Service-Portal für Zugriffsberechtigungen zurück

In 29 Prozent der Firmen gibt es ein Self-Service-Portal, über das die Nutzer selbst entscheiden können, welche Zugänge oder Zugriffsberechtigungen sie benötigen.

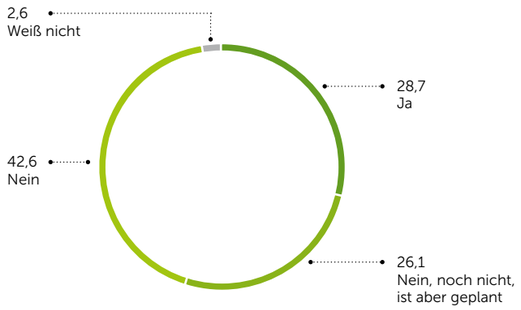
Vorreiter bei Self-Service-Portalen sind die Firmen, die über ein softwaregestütztes IAM verfügen (54 Prozent). Auch große und mittlere Unternehmen (41 bzw. 32 Prozent) tun sich hervor, in kleinen Firmen bis 100 Mitarbeiter hingegen setzen nur 14 Prozent auf ein Self-Service-Portal.

26 Prozent der befragten Unternehmen planen zumindest den Aufbau eines entsprechenden Portals.

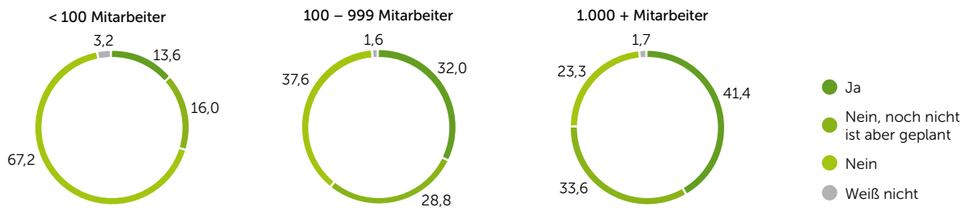
Nein zum Self-Service-Portal für die Einrichtung von Zugängen und Zugriffsberechtigungen sagen derzeit 43 Prozent der Unternehmen. Der Anteil der kleinen Firmen ist hier mit 67 Prozent überdurchschnittlich hoch.

Gibt es in Ihrem Unternehmen ein Self-Service-Portal, über das die Nutzer selbst entscheiden können, welche Zugänge oder Zugriffsberechtigungen sie benötigen?

Angaben in Prozent. Basis: n = 383



Ergebnis-Split nach Unternehmensgröße



9. Widersprüchliche Gefühle bei Super-User- und Administratoren-Zugängen

Drei Viertel der Firmen haben Super-User- und Administratoren-Zugänge mit erweiterten Zugriffsrechten eingerichtet, obwohl sie das damit verbundene Risiko sehen.

In 74 Prozent der Unternehmen gibt es sogenannte Super-User- und Administratoren-Zugänge mit weitreichenden Zugriffsrechten auf die Systeme.

Die Unterschiede zwischen kleinen, mittleren und großen Unternehmen sind hier marginal. Erstaunlich hoch ist mit 88 Prozent der Wert bei den Firmen mit softwaregestütztem IAM.

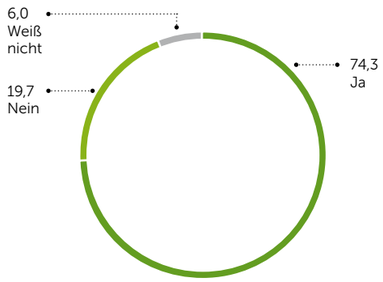
Die hohe Quote bei den Super-User- und Administratoren-Zugängen überrascht angesichts der Risiken, die Firmen damit verbinden.

Schließlich glauben 20 Prozent der Unternehmen, dass das Risiko dieser privilegierten Zugänge eindeutig zu groß sei; 44 Prozent sagen, dass es eher groß sei.

Nur 34 Prozent der Befragten sehen darin kein besonderes Risiko. Mit 41 Prozent zeigen sich hier die kleinen Unternehmen noch einmal deutlich entspannter als die mittleren (28 Prozent) und die großen (33 Prozent).

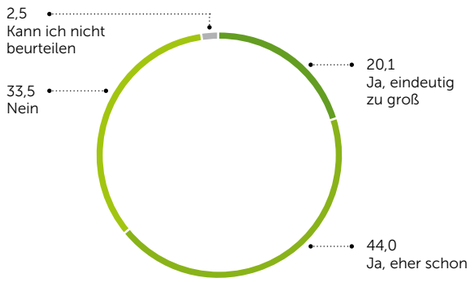
Gibt es in Ihrem Unternehmen sogenannte Super-User-/Administratorenzugänge?

Angaben in Prozent. Basis: n = 385



Glauben Sie, dass das Risiko solcher Super-User-/Administratorenzugänge zu groß ist?

Angaben in Prozent. Basis: n = 284 (Filter: nur Unternehmen, in denen es Super-User-und Administratorenzugänge gibt.)



Blick in die Zukunft

Identity- & Access-Management 2017

IAM: Es gibt noch viel zu tun für Unternehmen

Identity- & Access-Management (IAM), sprich die Verwaltung von Identitäten und deren Zugriffsrechten, ist zentral für die IT-Sicherheit und Compliance von Unternehmen. Mittlerweile geht es nicht mehr nur um die Verwaltung der Identitäten interner Mitarbeiter, sondern auch um die von externen Partnern, Kunden und Web-Services. Deutsche Firmen sind für diese neuen IAM-Herausforderungen nur teilweise gerüstet.

Von Jürgen Mauerer

„Früher" war die IAM-Welt noch überschaubar. Identity- & Access-Management (IAM) bestand bis vor wenigen Jahren vor allem aus der technischen Verwaltung von Benutzerkonten und Berechtigungen der eigenen Mitarbeiter im Unternehmen. Doch Digitalisierung, Cloud Computing und das Internet of Things (IoT) haben die Rolle von IAM verändert – und werden sie weiter verändern.

Da immer mehr Geschäftsmodelle und -prozesse direkt über das Internet vulgo die Cloud abgewickelt werden, müssen die IAM-Systeme jetzt auch verstärkt externe Partner und Kunden integrieren. Diese Dienstleister und Konsumenten müssen sich registrieren können, sie benötigen Zugriff auf Systeme, und die Benutzerkonten und Zugriffsrechte müssen verwaltet werden.

Viele Identitäten – die Komplexität steigt

Und dann ist da noch das Internet of Things mit einer Unmenge verbundener Geräte, Sensoren und „Dinge", die permanent miteinander kommunizieren. Aber sind all diese Identitäten tatsächlich vertrauenswürdig? Die Verwaltung sämtlicher Identitäten im IoT ist eine der zentralen Fragen für die Zukunft und alles andere als trivial. Firmen müssen diese Identitäten prüfen, die Laufzeit validieren und auch widerrufen können.

Die vorliegende IAM-Studie von COMPUTERWOCHE, CIO, TecChannel und ChannelPartner spiegelt diese neue Entwicklung wider. Zwar greifen in Firmen mit installierter IAM-Software vor allem die Mitarbeiter intern (75 Prozent) oder extern (60 Prozent) über Authentifizierungs- und Identitätsmanagement-Tools auf Systeme ihres Unternehmens zu. Doch bereits in 42 Prozent der Firmen erhalten Geschäftspartner, Dienstleister und Zulieferer (B2B) über IAM Zugang zum Netzwerk, in 23 Prozent die Kunden sowie Dienste und Services über Machine-to-Machine-Kommunikation (M2M), sprich über das IoT.

IAM ist wichtig für die Compliance

Mit der zunehmenden Vernetzung steigt natürlich auch die Zahl der möglichen Einfallstore für Hacker und andere Cyber-Kriminelle. Vertrauenswürdige Identitäten spielen daher eine umso wichtigere Rolle; Angreifer sollten keine Benutzerkonten übernehmen können. Das IAM-System muss unbefugte Zu-

griffe auf Netze und Applikationen abwehren sowie die Identitäten, Benutzerkonten und Zugriffsrechte von Tausenden bis Millionen von Nutzern verwalten. Es geht um Transparenz über die Benutzer, damit Unternehmen steuern können, welcher Nutzer mit welcher Authentifizierung welche Rechte erhält, und auch erkennen, wann Missbrauch vorliegt.

Eine derartige IAM-Infrastruktur minimiert die Sicherheitsrisiken und bildet gleichzeitig die tragende Säule, um regulatorische und Compliance-Anforderungen in Bezug auf Datenschutz erfüllen zu können. Nur wer eine einheitliche Sicht auf die Benutzer und deren Identitäten hat, kann Regeln konsequent umsetzen. Dies gilt vor allem für die EU-Datenschutz-Grundverordnung (EU-DSGVO), die am 25. Mai 2018 rechtswirksam in Kraft tritt. Ihre Umsetzung nennen die für die IAM-Studie befragten Unternehmen als größte Compliance-Herausforderung.

IAM: Deutsche Unternehmen haben Nachholbedarf

Doch die meisten deutschen Unternehmen sind noch nicht ausreichend auf die neuen IAM-Anforderungen vorbereitet. Das bestätigt die vorliegende Studie eindrucksvoll. Derzeit setzen nur rund 38 Prozent der befragten Firmen eine Softwarelösung für Identity- & Access-Management (IAM) ein. Vorreiter sind die großen Unternehmen mit einem Wert von 64 Prozent, gefolgt von den mittleren Firmen mit 39 Prozent. Nur 14 Prozent der kleinen Unternehmen nutzen eine IAM-Software. Immerhin 31 Prozent der Firmen planen den Einsatz einer IAM-Software. Hier müssen die deutschen Unternehmen nachziehen.

Gleiches gilt für Lösungen wie Single-Sign-On (SSO), Mobile Device Management (MDM) oder Security Information und Event Management (SIEM), die zukunftstaugliches IAM unterstützen und die Sicherheit erhöhen. Diese sind nur in rund einem Drittel der Unternehmen zu finden: SSO und MDM jeweils in 37 Prozent der Firmen, SIEM in 30 Prozent.

Zudem sollten die deutschen Unternehmen endlich die letzten Lücken bei der Multi-Faktor-Authentifizierung schließen. Denn etwas mehr als ein Fünftel der Firmen (21 Prozent) sichert ihre Zugänge zum Netzwerk derzeit NICHT über eine Multi-Faktor-Authentifizierung mit Token (Hardware, Software oder Push) ab. Auch hier sind vor allem die kleinen Unternehmen gefragt. Beim Thema „Zukunftssicheres IAM“ gibt es also noch viel zu tun.

Studiensteckbrief

Herausgeber	COMPUTERWOCHE, CIO, TecChannel und ChannelPartner
Studienpartner	**Platin-Partner:** procilon-IT Logistics GmbH TIMETOACT Software & Consulting GmbH **Silber-Partner:** Airlock by Ergon NEVIS Office Germany & Austria **Bronze-Partner:** Centrify KeyIdentity GmbH
Grundgesamtheit	Oberste IT- und Security-Verantwortliche von Unternehmen in der D-A-CH-Region: strategische (IT-)Entscheider im C-Level-Bereich und in den Fachbereichen (LoBs), IT-Entscheider und IT-Security-Spezialisten aus dem IT-Bereich
Teilnehmergenerierung	Stichprobenziehung in der IT-Entscheider-Datenbank von IDG Business Media, persönliche E-Mail-Einladungen zur Umfrage
Gesamtstichprobe	385 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	11. bis 21. Juli 2017
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung	IDG Research Services in enger Abstimmung mit den Studienpartnern
Durchführung	IDG Research Services
Technologischer Partner	Questback GmbH, Köln
Umfragesoftware	EFS Survey Spring 2017

Stichprobenstatistik

Branchenverteilung *	Land- und Forstwirtschaft, Fischerei, Bergbau	7,5 %
	Energie- und Wasserversorgung	11,2 %
	Chemisch-pharmazeutische Industrie	9,6 %
	Metallerzeugende und -verarbeitende Industrie	9,1 %
	Maschinen- und Anlagenbau	11,7 %
	Automobilindustrie und Zulieferer	7,8 %
	Herstellung von elektrotechnischen Gütern, IT-Industrie	12,7 %
	Konsumgüter-, Nahrungs- und Genussmittelindustrie	3,6 %
	Medien, Papier- und Druckgewerbe	3,6 %
	Baugewerbe, Handwerk	6,5 %
	Groß- und Einzelhandel (inklusive Online-Handel)	9,9 %
	Banken und Versicherungen	11,7 %
	Transport, Logistik und Verkehr	9,6 %
	Hotel- und Gastgewerbe, Tourismus	7,8 %
	Dienstleistungen für Unternehmen	19,7 %
	Öffentl. Verwaltung, Gebietskörperschaften, Sozialversicherung	6,8 %
	Gesundheits- und Sozialwesen	4,9 %
	Schule, Universität, Hochschule	5,2 %
	Andere Branchengruppe	9,6 %
Unternehmensgröße	Weniger als 100 Beschäftigte	34,2 %
	100 bis 999 Beschäftigte	34,2 %
	1.000 bis 9.999 Beschäftigte	24,5 %
	10.000 Beschäftigte und mehr	7,1 %
Umsatzklasse	Weniger als 100 Millionen Euro	45,3 %
	100 bis 999 Millionen Euro	28,6 %
	1 Milliarde Euro und mehr	26,1 %
Jährliche Aufwendungen in IT-Systeme sowie Anwendungen/Applikationen		
	Weniger als 1 Million Euro	43,3 %
	1 bis 10 Millionen Euro	30,9 %
	10 bis 100 Millionen Euro	19,8 %
	100 Millionen Euro und mehr	5,9 %

* Mehrfachnennungen möglich

procilon – Die sichere Lösung

Die procilon Unternehmensgruppe mit Sitz in Taucha bei Leipzig und Niederlassungen in Berlin und Dortmund ist einer der führenden Komplettanbieter von Public-Key-Infrastructure-Lösungen für Unternehmen, Institutionen und öffentliche Einrichtungen. Eigenentwickelte Softwareprodukte sichern seit mehr als 15 Jahren digitale Identitäten und Datenaustausch ab und sorgen für die rechtskonforme Aufbewahrung wichtiger Daten in elektronischer Form.

Abgeleitet vom individuell geforderten Schutzbedarf realisiert procilon mithilfe intelligenter Sicherheitssoftware und Integrationskomponenten ein hohes Niveau der Informationssicherheit sowie die automatisierte Einhaltung von Datenschutz, Datensicherheit und Vertrauenswürdigkeit.

Das Produktspektrum reicht von einfacher Dateiverschlüsselung im Browser über Signaturanwendungen, Access- und Identity-Management bis hin zu kompletten Public Key Infrastrukturen für Vertrauensdiensteanbieter nach EU-eIDAS-Verordnung. Der Schutz digitaler Identitäten, der rechtskonforme, authentische und nachweisbare Austausch elektronischer Daten steht ebenso im Fokus wie die Erhaltung eines hohen Beweiswertes bei der Langzeitarchivierung. Vielfältige sichere Services aus der Cloud runden das Portfolio ab.

Die Softwareentwicklung und Produkte von procilon wurden durch den TÜV-IT auditiert und nach Common Criteria EAL 4+ VAN5 (Angriffspotenzial hoch) zertifiziert. Darüber hinaus erteilte das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Zertifizierung für die Lösung zur Langzeitarchivierung qualifiziert signierter Dokumente.

Seit 2013 ist procilon vom Bundesministerium für Justiz mit der Pflege und Weiterentwicklung des Verzeichnisdienstes SAFE (Secure Access to Federated e-Justice/e-Government), der für eine einheitliche Kommunikationsinfrastruktur im elektronischen Rechtsverkehr sorgt, beauftragt. Im Jahr 2014 implementierte procilon die notwendigen technischen Komponenten für den Betrieb des TrustCenters der Bundesnotarkammer, im Jahr 2016 folgte das Deutsche Gesundheitsnetz.

Mit procilon-Komponenten können Lösungen von der Erzeugung elektronischer Zertifikate und Signaturen, deren Verwaltung und Prüfung bis hin zu unterschiedlichen Verschlüsselungs- und Authentisierungsszenarien realisiert werden.

Ferner begleitet procilon Unternehmen bei vorgeschriebenen Sicherheitszertifizierungen zum Schutz kritischer Infrastrukturen. Beratungsleistungen durch projekterfahrene Mitarbeiter und zertifizierte Auditoren unterstützen bei der Implementierung von IT-Sicherheits-Management-Systemen (ISMS) insbesondere im Rahmen der ISO Normen.

Über 1.000 Kunden aus dem Öffentlichen Dienst, Versorgungsunternehmen, Industrie und Mittelstand vertrauen auf die langjährige IT-Sicherheits-Expertise von procilon. Die Aktualität und Praxisnähe seiner Lösungen stellt procilon durch die Mitarbeit in Branchen- und Technologieverbänden sicher. Resonanz aus langfristigen Kundenbeziehungen und Synergien innovativer Partnerschaften versetzen procilon in die Lage, sowohl leistungsfähige Security-Standardprodukte „made in Germany“ zu entwickeln als auch branchenspezifische Individuallösungen zu konzipieren und umzusetzen.

procilon GROUP

procilon-IT Logistics GmbH
Leipziger Straße 110
04425 Taucha
www.procilon.de

Torsten Rienaß, Geschäftsführer der procilon IT-Logistics GmbH

„Im Zeitalter der Digitalisierung ist der Schutz elektronischer Identitäten nicht hoch genug einzustufen. Hier muss in erster Linie Vertrauen und Transparenz geschaffen werden, denn ohne Vertrauen sind weder vollständig digitale Geschäftsprozesse noch ein funktionierendes IoT möglich.

Als Anbieter von softwaregestütztem Identity- & Access-Management sehen wir uns hier in der Pflicht, die passenden Lösungen auf einem hohen Sicherheitsniveau bereitzustellen.“

Felix Binsack
Geschäftsführer
TIMETOACT GROUP

Hermann Ballé
Geschäftsführer
TIMETOACT GROUP

TIMETOACT GROUP

Es gibt nichts Gutes, außer man tut es!

Die TIMETOACT GROUP bietet Beratungsleistungen und IT-Lösungen auf Basis von Software von IBM, Microsoft, Oracle, Google sowie weiterer Partner und offenen Standards an.

In der TIMETOACT GROUP sind sechs Marken der Software- und Consulting-Branche unter einem Dach vereint, die eng zusammenarbeiten: BLUETRADE, CLOUDPILOTS, edcom, novaCapta, TIMETOACT und X-INTEGRATE.

1998 gegründet, beschäftigt sie heute über 280 Mitarbeiter an sieben Standorten in Deutschland und Vertriebsniederlassungen in Österreich, der Schweiz und den Niederlanden.

In der Business Unit Identity & Access Governance unterstützt die TIMETOACT GROUP ihre Kunden bei der Erstellung ganzheitlicher Identity- & Access-Management-Strategien wie auch deren Umsetzung und Betreuung.

Mit Unterstützung mehrerer Technologiepartner können State-of-the-Art-Solutions anhand des konkreten Bedarfs des Kunden realisiert werden. Bei der Umsetzung werden stets die notwendigen Governance-Funktionen berücksichtigt.

Die TIMETOACT GROUP hat dabei ihr Vorgehensmodell über Jahre hinweg entwickelt und optimiert. Anhand eines Reifegradmodells können jederzeit Status und Erfolg der IAM-Strategie gemessen werden. So wird dem Kunden eine automatisierte und revisionssichere Lösung geboten, die alle Anforderungen an Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Nachvollziehbarkeit erfüllt.

Auch nach Fertigstellung der Lösung wird der Kunde nicht alleine gelassen. Die TIMETOACT GROUP garantiert durch ein Managed-Services-Paket weitere Unterstützung nach Umsetzung der IAG/IAM-Applikation.

TIMETOACT GROUP
SOFTWARE & CONSULTING

TIMETOACT Software & Consulting GmbH
Im Mediapark 5c
50670 Köln

www.timetoact-group.de

Eigenes IAG-Team unterstützt von der Idee bis zur Umsetzung mit anschließendem Managed Service

Das Expertenteam des Kölner Unternehmens verfügt über langjährige Erfahrung aus einer Vielzahl von Projekten insbesondere in regulierten Branchen.

Der Kunde wird bereits bei der Evaluierung und Auswahl geeigneter Produkte unterstützt.

Auf den Bedarf des Auftraggebers abgestimmt leistet die TIMETOACT GROUP die fachliche und technische Konzeption sowie deren Umsetzung bis hin zum Betrieb.

Anschließend werden als Managed Service die Weiterentwicklung und die Pflege der Lösung gewährleistet.

Impressum / Kontakt / Studienreihe

Identity- & Access-Management 2017

Herausgeber:

IDG Business Media GmbH

Anschrift
Lyonel-Feininger-Str. 26
80807 München
Telefon: +49 89 36086 – 0
Fax: +49 89 36086 – 118
E-Mail: info@idgbusiness.de

Vertretungsberechtigter
York von Heimburg
Geschäftsführer

Registergericht
Amtsgericht München
HRB 99187

Umsatzsteueridentifikations-
nummer: DE 811 257 800

Weitere Informationen unter:
www.idg.de

Platin-Partner:

procilon-IT Logistics GmbH
Leipziger Straße 110
04425 Taucha
Telefon: +49 34298 4878 – 31
E-Mail: anfrage@procilon.de
Web: www.procilon.de

TIMETOACT
Software & Consulting GmbH
Im Mediapark 5c
50670 Köln
Telefon: +49 221 97343 0
E-Mail: info@timetoact.de
Web: www.timetoact-group.de

Silber-Partner:

Airlock by Ergon
Merkurstrasse 43
8032 Zürich
Schweiz
Telefon: +41 44 268 89 00
E-Mail: info@airlock.com
Web: www.airlock.com

NEVIS
NEVIS Office Germany & Austria
Hubenstein 11
84416 Taufkirchen/Vils
Telefon: +49 8084 41331 0
E-Mail: info@nevis-security.de
Web: www.nevis-security.de

Bronze-Partner:

Centrify
Lily Hill House, Lily Hill Road 1
RG12 2SJ Bracknell, Berkshire
United Kingdom
Telefon: +44 1344 317955
E-Mail: emeamarketing@centrify.com
Web: www.centrify.com

KeyIdentity GmbH
Robert-Koch-Straße 9
64331 Weiterstadt
Telefon: +49 6151 860860
E-Mail: info@keyidentity.com
Web: www.keyidentity.com

Studienkonzept / Fragebogenentwicklung:
Matthias Teichmann,
IDG Research Services

Endredaktion / CvD Studienberichtsband:
Mareile Reisch, Hamburg
Matthias Teichmann,
IDG Research Services

Analysen / Kommentierungen:
Jürgen Mauerer, München

Umfrage-Programmierung:
Thamar Thomas-Ißbrücker,
IDG Research Services
auf EFS Survey Spring 2017

Grafik:
Patrick Birnbreier, München

Umschlagkonzept:
Sandra Schmitt,
IDG Research Services
(unter Verwendung eines Farbfotos für Vorder- und Rückseite von © shutterstock.com / Titima Ongkantong

Lektorat:
Dr. Renate Oettinger,
München

Druck:
Peradruck GmbH
Hofmannstr. 7b
81379 München

Ansprechpartner:
Matthias Teichmann
Director Research
IDG Research Services
Telefon: +49 89 36086 – 131
mteichmann@idgbusiness.de

Der Autor dieser Studie

Jürgen Mauerer
Jürgen Mauerer arbeitet seit Oktober 2002 als freiberuflicher IT-Fachjournalist in München. Er schreibt vorwiegend über aktuelle Themen und Trends rund um IT und Wirtschaft für Publikationen wie COMPUTERWOCHE, com! professional oder ZD.NET. Darüber hinaus berät und unterstützt er PR-Agenturen sowie IT-Unternehmen bei der Erstellung von Anwenderberichten, Whitepapers, Fachartikeln oder Microsites und moderiert Podiumsdiskussionen und Veranstaltungen.

Unser Autorenteam

Alex Jake Freimark
Alex Jake Freimark wechselte 2009 von der Redaktion der COMPUTERWOCHE in die Freiberuflichkeit.
Er schreibt für Medien und Unternehmen, sein Auftragsschwerpunkt liegt im Corporate Publishing. Dabei stehen technologische Innovationen im Fokus, aber auch der Wandel von Organisationen, Märkten und Menschen.

Christoph Lixenfeld
Christoph Lixenfeld schreibt seit 25 Jahren als Journalist und Autor für die Süddeutsche Zeitung, den Spiegel, Focus, den Tagesspiegel, das Handelsblatt, die Wirtschaftswoche, COMPUTERWOCHE und viele andere. Außerdem macht er Hörfunk, vor allem für DeutschlandRadio, und produziert TV-Beiträge, zum Beispiel für die ARD-Magazine Panorama und Plusminus. Inhaltlich geht es häufig um die Themen Wirtschaft und IT, aber nicht nur.

Bernd Reder
Bernd Reder ist seit rund 30 Jahren als Fachjournalist für Medien, PR-Agenturen und Unternehmen tätig. Zu seinen thematischen Schwerpunkten zählen die Informations- und Netzwerktechnik, Cloud Computing, IT-Security und Mobility. Bevor er sich selbstständig machte, war Reder in den Redaktionen führender Fachpublikationen tätig. Dazu zählen Elektronik, Network World, Digital World und Network Computing.

Michael Schweizer
Michael Schweizer ist freier Redakteur und Autor in München. Oft schreibt er über Menschen, Personal- und Karrierefragen mit IT-Bezug. Besonders interessiert ihn alles, was mit Wissenschaft zu tun hat, also zum Beispiel unabhängige Studien zu komplizierten Themen. Als freier Schlussredakteur ist er unter anderem für die Print-Ausgaben der IDG-Publikationen COMPUTERWOCHE, CIO und ChannelPartner zuständig. Er übernimmt auch Buchlektorate.

Sales-Team

Carolin Beck
Account Manager Research
IDG Research Services
Telefon: 089 36086 – 122
cbeck@idgbusiness.de

Franziska Kaufmann
Account Manager Research
IDG Research Services
Telefon: 089 36086 – 882
fkaufmann@idgbusiness.de

Jessica Schmitz-Nellen
Account Manager Research
IDG Research Services
Telefon: 089 36086 – 745
jschmitz-nellen@idg.de

Gesamtstudienleitung

Matthias Teichmann
Director Research
IDG Research Services
Telefon: 089 36086 – 131
mteichmann@idgbusiness.de

Unsere Studienreihe

Vorschau Studienreihe

November 2017:
Internet of Things

Dezember 2017:
IT-Service-Management

Februar 2018:
4digital

Februar 2018:
IT-Freiberufler

März 2018:
Cloud Migration

April 2018:
Machine Learning / Deep Learning

Mai 2018:
Predictive Analytics

Mai 2018:
Sourcing

Juni 2018:
Arbeitsplatz der Zukunft

Juli 2018:
IAM-as-a-Service

August 2018:
Legacy-Modernisierung

September 2018:
Managed Security

Die initialen redaktionellen Round Tables finden jeweils rund drei bis vier Monate vor den Veröffentlichungsterminen statt.

(Planungsstand 31.8.2017, Änderungen vorbehalten)

Erhältlich in unserem Studien-Shop auf
www.computerwoche.de/studien

Laufende Studienberichterstattung auf
www.computerwoche.de/p/research,3557