COMPUTERWOCHE CIO ChannelPartner TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE IDENTITY- & ACCESS-MANAGEMENT 2017

DIE WICHTIGSTEN KEY FINDINGS

PRÄSENTIERT VON AIRLOCK BY ERGON

AIRLOCK by ergon

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

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).

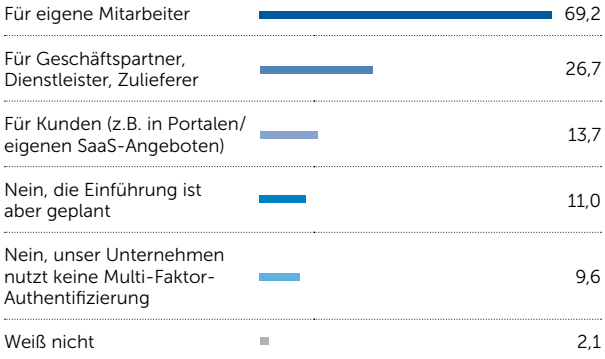
In 27 Prozent der Unternehmen müssen sich Geschäftspartner, Dienstleister und Zulieferer auf mehreren Wegen authentifizieren. Nur 6 Prozent der kleinen Unternehmen haben dies auf ihrer Agenda.

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).

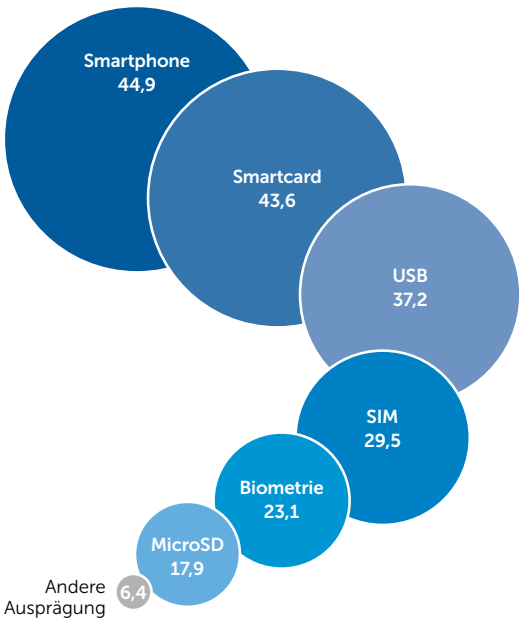
Nutzt Ihr Unternehmen für die Absicherung der Zugänge eine Multi-Faktor-Authentifizierung mit Token (Hardware, Software oder Push)?

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)



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

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.

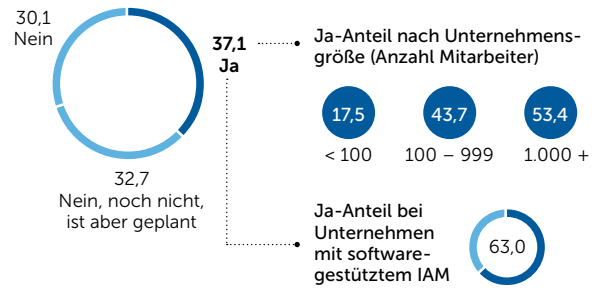
Nur 37 Prozent der befragten Firmen setzen eine SSO-Lösung für die einfachere Anmeldung bei ihren Systemen ein. Die Nase vorn haben hier die großen Firmen mit 53 Prozent, während nur 18 Prozent der kleinen Unternehmen SSO nutzen. Absolute SSO-Vorreiter mit 63 Prozent sind hier die Unternehmen, die bereits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

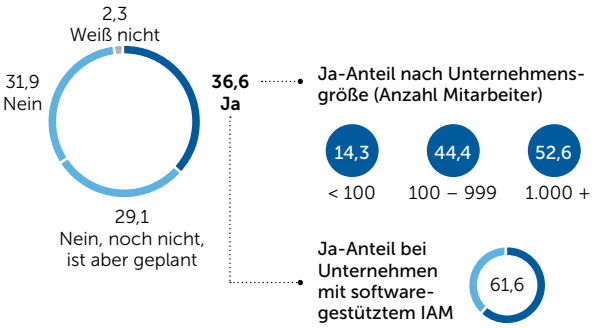
Gibt es für die Mitarbeiter Ihres Unternehmens eine Single-Sign-On (SSO)-Lösung?

Angaben in Prozent. Basis: n = 385



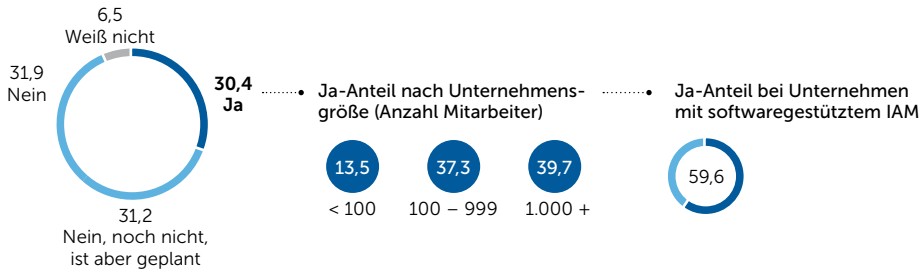
Setzt Ihr Unternehmen eine MDM-Lösung ein (Mobile Device Management)?

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



Über Ergon Informatik AG und Airlock Suite

Die Airlock Suite kombiniert die Themen Filterung und Authentisierung in einer abgestimmten Gesamtlösung, die punkto Usability und Services Maßstäbe setzt. Die Airlock WAF (Web Application Firewall) schützt Internet-Anwendungen zuverlässig mit systematischen Kontroll- und Filterungsmechanismen und mit vielfältigen Erweiterungsoptionen.

Im Zusammenspiel mit Airlock WAF ermöglicht Airlock Login die zuverlässige Authentisierung und Autorisierung von Benutzern. Doch Airlock Login steht nicht nur für optimale Sicherheit, sondern auch für hohe Usability und Kosteneffizienz.

Airlock IAM ist die zentrale Authentifizierungsplattform mit Enterprise-Funktionen. Sie ermöglicht Kunden, Partnern oder Mitarbeitenden mit einmaliger Anmeldung den sicheren Zugang zu Daten und Anwendungen und automatisiert die Benutzeradministration.

Airlock ist Teil der 1984 gegründete Ergon Informatik AG und führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten.

Die Basis für unseren Erfolg: 270 hoch qualifizierte IT-Spezialisten, die dank herausragendem Know-how neue Technologietrends antizipieren und mit innovativen Lösungen Wettbewerbsvorteile sicherstellen. Ergon realisiert hauptsächlich Großprojekte im B2B-Bereich.

AIRLOCK by ergon

Herausgeber:
IDG Business Media GmbH
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

Umsatzsteueridentifikationsnummer: DE 811 257 800

Weitere Informationen unter:
www.idg.de

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

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

Grafik:
Patrick Birnbreier, München

Lektorat:
Dr. Renate Oettinger,
München

Druck:
Peradruck GmbH
Hofmannstr. 7b
81379 München

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 Winter 2017