WISSEN,
DAS ANKOMMT.

Leseprobe zum Download

Liebe Besucherinnen und Besucher unserer Homepage,

tagtäglich müssen Sie wichtige Entscheidungen treffen, Mitarbeiter führen oder sich technischen Herausforderungen stellen. Dazu brauchen Sie verlässliche Informationen, direkt einsetzbare Arbeitshilfen und Tipps aus der Praxis.

Es ist unser Ziel, Ihnen genau das zu liefern. Dafür steht seit mehr als 25 Jahren die FORUM VERLAG HERKERT GMBH.

Zusammen mit Fachexperten und Praktikern entwickeln wir unser Portfolio ständig weiter, basierend auf Ihren speziellen Bedürfnissen.

Überzeugen Sie sich selbst von der Aktualität und vom hohen Praxisnutzen unseres Angebots.

Falls Sie noch nähere Informationen wünschen oder gleich über die Homepage bestellen möchten, klicken Sie einfach auf den Button „In den Warenkorb“ oder wenden sich bitte direkt an:

FORUM VERLAG HERKERT GMBH
Mandichostr. 18
86504 Merching
Telefon: 08233 / 381-123
Telefax: 08233 / 381-222

E-Mail: service@forum-verlag.com
www.forum-verlag.com

© Alle Rechte vorbehalten. Ausdruck, datentechnische Vervielfältigung (auch auszugsweise) oder Veränderung bedürfen der schriftlichen Zustimmung des Verlages.

Zutrittskontrolle
Unbefugten muss der Zutritt zu Datenverarbeitungsanlagen verwehrt werden, z. B. durch Türschlösser, Alarmanlagen oder abschließbare Aktenschränke. Sobald Sie einen Raum verlassen, verstauen Sie sensible Dokumente sorgfältig und schließen Sie die Schränke oder den Raum ab.

Zugriffskontrolle
Stellen Sie sicher, dass Schutzmechanismen wie Berechtigungen, automatische Sperren und Verschlüsselung angewendet werden und aktiv sind (z. B. E-Mail-, SSL-Verschlüsselung bei Formularen auf Websites).

Auch der **„Clean Desk"** ist ein hilfreicher und gleichzeitig ganz einfacher Beitrag zu Datensicherheit und Vertraulichkeit:

- Aufräumen: Stellen Sie sich selbst die Frage: „Muss das hier wirklich rumliegen?"
- Abschließen: Bei längerer Abwesenheit sollten Sie zudem Unterlagen und Datenträger mit personenbezogenen Daten etc. im Schrank/Rollcontainer einschließen und den Schlüssel sicher verwahren.

▶ **Passwörter**
Fragen Sie Ihren Vorgesetzten nach einer bestehenden Policy zum Erstellen sicherer Passwörter. Geben Sie Passwörter nie heraus und achten Sie auf eine sichere Aufbewahrung (also keine Zettel am Monitor oder unter der Tastatur!). Und denken Sie daran, dasselbe Passwort nicht mehrmals zu verwenden!

Die Sicherheit Ihrer Passwörter ist entscheidend. „1234", „qwertz" oder „Hallo" scheiden hier definitiv aus. Verwenden Sie stattdessen z. B. eine Passphrase in Verbindung mit einem Datum.

Beispiel:
Aus „Ein Konzept für Datenschutz am Arbeitsplatz ist wichtig!" wird dann: 1KfDaAiw!
Hier können noch Monat und Jahreszahl angehängt werden: 1KfDaAiw!12-2017

▶ **Computer- und Bildschirmsperre**
Jeder PC-Arbeitsplatz und jedes Notebook muss beim Start eine Passwortabfrage bereithalten, um den Zugriff von Unberechtigten auszuschließen. Achten Sie gerade hier auf ein sicheres Passwort. Auch wenn Sie den Arbeitsplatz nur kurz verlassen, sollten Sie den Bildschirmschoner mit Passwort aktivieren (Windows-Rechner: WINDOWS-Taste + L; Mac-Rechner: Control + Shift + Eject). Zusätzlich sollte nach 20–30 min. eine solche Bildschirmsperre automatisch einsetzen.

▶ **Verschlüsselte Festplatte**
Wenn Sie mobile Geräte wie Notebooks etc. verwenden, sollten Sie die IT-Abteilung darauf ansprechen, ob die Festplatte verschlüsselt worden ist und ob im Verlustfall eine Fernlöschung möglich ist.

▶ **Datenschutzfolie für Monitore und Notebooks**
Gerade beim mobilen Arbeiten gewähren Sie häufig Sitznachbarn im Zug, Bus etc. ungewollt Einblicke in sehr empfindliche Dokumente. Nutzen Sie daher eine sog. Datenschutzfolie für Monitore.

▶ **Schutz vor Mithören**
Datenschutz gilt auch für Telefonate im öffentlichen Raum. Sorgen Sie also dafür, dass Unbefugte keine Telefongespräche mitverfolgen können.

▶ **Aktenvernichter – ein Muss?**
Dokumente mit empfindlichen oder personenbezogenen Daten und Geschäftsgeheimnissen, die entsorgt werden sollen, gehören immer in einen Aktenvernichter (Sicherheitsstufen vgl. DIN 66399).

▶ **Gefahr durch Social Engineering und Spoofing/Phishing**
„Virtuelle Haustürbetrüger" versuchen, durch Anrufe oder Nachrichten im vermeintlichen Auftrag von Vorgesetzten, Kundenunternehmen oder Bekannten an vertrauliche Infos bzw. sensible Daten zu gelangen oder die Opfer zum Öffnen von Dateien bzw. zur Installation von Programmen zu verleiten. Auch gefälschte E-Mails und Internetseiten („Phishing") dienen Cyber-Kriminellen, an vertrauliche Daten wie Zugangsdaten oder Kreditkartennummern heranzukommen.

WISSEN,
DAS ANKOMMT.

Bestellmöglichkeiten

Mitarbeiter-Merkblatt
Datenschutz und IT-Sicherheit

Für weitere Produktinformationen oder zum Bestellen hilft Ihnen unser Kundenservice gerne weiter:

Kundenservice

Telefon: 08233 / 381-123
E-Mail: service@forum-verlag.com

Oder nutzen Sie bequem die Informations- und Bestellmöglichkeiten zu diesem Produkt in unserem Online-Shop:

Internet

https://www.forum-verlag.com/details/index/id/10035

FORUM VERLAG HERKERT GMBH, Mandichostraße 18, 86504 Merching,
Tel.: (08233) 381 123, E-Mail: service@forum-verlag.com, Internet: www.forum-verlag.com