Das comTeam Kunden-Magazin.

Ausgabe Juni 2018

EF.IT

ERFOLGSFAKTOR-IT

DSGVO

Die EU-DSGVO greift - was tun, wenn man sich noch nicht darauf eingestellt hat?

Industrie 4.0 | Seite 8
Neue Lösungen gegen neue Bedrohungen durch IoT

VR-Headsets | Seite 10
Warum sich Unternehmen für Virtual Reality interessieren sollten.

Multifaktor-Authentifizierung | Seite 13
Schlüssel zu mehr Sicherheit

© Vasily Merkushev - #200491765 - Fotolia.com

WIR DIGITALISIEREN ZUKUNFT

comTeam DAS TECHNOLOGIE-NETZWERK

Weiterbildung für Führungskräfte, Vertiebsmitarbeiter, Techniker & Auszubildene im Systemhausgeschäft

Wissen von Profis für IT Profis.

Chance nutzen und anmelden, jetzt!

comTeam stellt eine Schulungsplattform unter https://seminare-comteam.de bereit. Das Besondere ist, dass nicht nur Seminare aus IT und TK angeboten werden. Es werden unternehmensbegleitende Bereiche wie Recht, Personalentwicklung, Betriebswirtschaft, Kommunikation u.v.m. abgebildet.

Die Plattform ist nicht nur für die Mitglieder im Verbund, sondern auch für interessierte Systemhausbetreiber offen. Die Vereinfachung der Suche nach qualifizierten Seminaren gelingt mit der Bündelung aller Angebote auf einer einzigen zentralen Plattform. Das Programm umfasst aktuell rund 800 Angebote.

Besonders beliebt sind derzeit vor allem Seminare aus dem Bereich Vertrieb, aber auch jene, die den Wandel vom klassischen Systemhaus zum IT-Consultant beraten. Aber auch Schulungen, die auf die neue Europäische Datenschutzverordnung im Mai 2018 vorbereiten, werden aktuell verstärkt gebucht.

Seminare für die DSGVO:
https://comteam-seminare.de/seminar.php?id=5761
https://comteam-seminare.de/seminar.php?id=5191

Seminare für den Datenschutzbeauftragten an mehreren Terminen: **https://comteamseminare.de/seminar.php?id=5756**

KONTAKT
comTeam Systemhaus GmbH
Mündelheimer Weg 40 - 40472 Düsseldorf
Telefon 0211 . 4156 767
fkautz@comteam.de

comTeam DAS TECHNOLOGIE-NETZWERK

© blackzheep - #165874373 - Fotolia.com

EDITORIAL

Liebe Leserinnen und Leser,

herzlich willkommen zur Sommerausgabe Juni/Juli 2018 der EFIT. Wir freuen uns ganz besonders, denn diese Ausgabe strahlt nicht nur mit tollen Themen sondern auch mit einem neuen Design. Die EFIT soll für Sie Leser immer auf einem topaktuellen Stand sein und das natürlich nicht nur in Bezug auf die Themen, sondern auch auf das Design.

Aus diesem Grund ist in die Artikelauswahl dieser Ausgabe auch die EU- DSGVO gefallen, die nun bereits seit dem 25. Mai 2018 greift. Das Titelthema verrät Ihnen im Interview mit einem zertifizierten Datenschutzbeauftragten, was Sie kurzfristig noch machen können und sollten. Außerdem wird erläutert, was sich im einzelnen geändert hat. **Tipp:** Lesen Sie sich doch mal auf Seite 2 das Advertorial durch, die Schulungsplattform von comTeam bietet Schulungen speziell zur DSGVO an.

Wie sichern Sie die Computer in Ihrem Unternehmen ab, mit einem einzigen Passwort oder haben Sie bereits die Multifaktor Authentifizierung eingeführt? Der Artikel „Schlüssel zu mehr Sicherheit“ führt Ihnen im Interview mit einem echten Experten die großen Sicherheitsunterschiede auf.

Bei dem Thema Virtual Reality denken wahrscheinlich sehr viele an die Gaming-Szene, der Geschäftsbereich dieser Technik ist dennoch viel interessanter. Hier ist sehr viel möglich, jedoch möchten wir noch nicht zu viel vorwegnehmen.

Ich wünsche Ihnen, auch im Namen der Redaktion, viel Freude beim Lesen. Selbstverständlich stehen wir Ihnen als Ansprechpartner zu allen Fragen der EFIT gerne zur Verfügung. Über Ihre Anregungen und Themenvorschläge, die Sie gerne an **partner@comteam.de** senden können, sind wir immer dankbar.

Sven Glatter
Geschäftsführer
comTeam Systemhaus GmbH

INHALTSVERZEICHNIS

2 **Advertorial**
Wissen von Profis für Profis

4 **EU-DSGVO greift** - was tun, wenn man sich noch nicht darauf eingestellt hat?

5 **Mobillfunk der 5. Generation**
Erstes G5-Netz Europas gestartet

8 **Industrie 4.0**
Neue Lösungen gegen neue Bedrohungen durch IoT

10 **VR-Headsets** - Warum sich Unternehmen für Virtual Reality interessieren sollten

12 **Gesundheit**
Fitness-Übungen fürs Büro, die niemand bemerkt

13 **Multifaktor-Authentifizierung**
Schlüssel zu mehr Sicherheit

14 **Recruiting**
Interesse an Arbeitgeber-Bewertungen online steigt!

IMPRESSUM

Herausgeber
comTeam Systemhaus GmbH
Mündelheimer Weg 40
40472 Düsseldorf

Redaktion / Kontakt
Elena Siala (esiala@comteam.de)
Telefon 02 11 / 41 56 - 386

Autoren
Folker Lück, tellyou Redaktionsbüro 02 11 / 159 608 64
Viermann - die Redaktion für Wissenschaft und Technik,
Telefon 02 21 / 271 67 370
PR Laxy - Arno Laxy, Telefon 089 / 159 296 61

Urheberrecht
Dieses Werk ist urheberrechtlich geschützt. Jede Vervielfältigung ist ohne schriftliche Zustimmung der Redaktion unzulässig. Alle Angaben ohne Gewähr.

Satz und Druck
Werbeatelier - Stefan Dammer, info@atelier-dammer.de

Inserenten
D-LINK - www.dlink.com
comTeam - www.comteam.de

© XtravaganT - #201123071 - Fotolia.com

Die EU-DSGVO greift - was tun, wenn man sich noch nicht darauf eingestellt hat?

Der Tag X ist vorbei und die Welt steht noch. Das eigene Unternehmen ist nicht wegen Datenschutzmängeln verklagt worden. Alles gut also? Kommt drauf an. Die Datenschutzgrundverordnung (DSGVO) ist seit dem 25. Mai 2018 rechtswirksam. Bei Nichtbefolgen drohen potenziell abschreckend hohe Strafen. Diejenigen, die sich auf die Verordnung vorbereitet haben, können aus gutem Grund ruhig bleiben. Diejenigen aber, die bisher nichts getan haben, um ihr Unternehmen fit zu machen für diese grundlegende europaweite Neuregelung des Datenschutzes, sollten schleunigst anfangen. Denn, dass sie bis jetzt nicht von den Aufsichtsbehörden belangt wurden, liegt im Zweifel nur daran, dass sie noch nicht an der Reihe sind.

Mit dem Datenschutz Ernst machen und zwar (EU)-europaweit einheitlich wollen die Schöpfer dieser neuen Verordnung. Betrachtet man die mediale Aufregung in den letzten Monaten so ist es ihnen sicherlich gelungen, den Schutz personenbezogener Daten in den Blick der Öffentlichkeit zu bringen. Inwieweit die Unternehmen am 25. Mai aber reagiert und ihre Hausaufgaben gemacht haben, steht auf einem anderen Blatt. Gewiss ist, dass bis zuletzt allzu oft nichts geschehen ist. So haben zum Beispiel noch Ende März 70 Prozent der Top-50-Onlineshops die Anforderungen der Verordnung nicht erfüllt. Das ergab eine Analyse von Usercentrics. Damit der Datenschutz kein Papiertiger (mehr) ist, ahnden die Aufsichtsbehörden dessen Missachtung jetzt mit abschreckend hohen Strafen von bis zu vier Prozent vom Jahresumsatz bzw. maximal einer Summe von 20 Millionen Euro. Die gute Nachricht für alle kleinen und mittelständischen Unternehmen (KMU), die noch nichts in Sachen DSGVO getan haben, ist, dass ihnen noch etwas Zeit bleibt bis die Behörden sie überprüfen. Denn die wenden sich zunächst den großen Fischen zu. *„Pragmatisch betrachtet werden die KMU, besonders die mit bis 100 Mitarbeitern, nicht so schnell in den Fokus der Aufsichtsbehörden geraten. Eher ist zu befürchten, dass Abmahnanwälte wieder zuschlagen“*, erläutert René Floitgraf, zertifizierter Datenschutzbeauftragter und Geschäftsführer des IT-Dienstleisters Spider Network Consulting GmbH, Aachen.

Vor Abmahnanwälten wird gewarnt

Abmahnanwälte haben im Zweifel schon begonnen, nach Angriffsflächen im Außenauftritt von Unternehmen zu suchen. Die Firmenwebsite muss die geforderten Datenschutzinformationen enthalten und

© 755009773 – shutterstock

Erstes 5G-Netz Europas gestartet!

Der Mobilfunk der 5. Generation wird ein Highspeed-Datennetz. Viele Anwendungen in den Bereichen Internet of Things, Industrie 4.0 und Autonomes Fahren werden dadurch erst möglich. In der Berliner City hat die Telekom jetzt das europaweit erste 5G-Netz gestartet, das den künftigen Kommunikationsstandard vollständig unterstützt.

Der heutige 4G-Mobilfunk auf Basis von LTE bietet bereits glasklare Sprachverbindungen und ermöglicht eine Breitband-Datenübertragung. Der entscheidende Schritt bei den ab 2020 startenden 5G-Mobilfunknetzen wird sein, dass die Latenzzeiten massiv sinken und mehr Nutzern zeitgleich noch höhere Datenraten zur Verfügung stehen. Damit können Daten quasi in Echtzeit übertragen werden. Das mag für „Otto Normalverbraucher“ (fast) uninteressant sein, aber für Anwendungen im Bereich Industrie 4.0 oder die Steuerung autonomer Fahrzeuge ist dieser Schritt essentiell.

Auf dem Weg zur nächsten Mobilfunkgeneration ist die Deutsche Telekom jetzt einen entscheidenden Schritt weitergekommen: Sie hat in Berlin die erste 5G-Datenverbindung Europas im Livebetrieb gestartet. Aktuell baut der Konzern im Berliner Zentrum ein 5G-Cluster auf. Das 5G Cluster hat im ersten Schritt eine Breite von rund fünf Kilometern. Aktuell sind in den Stadtteilen Mitte und Schöneberg die ersten sechs kommerziellen Antennen im Testbetrieb. Im Laufe des Sommers werden 70 Antennen an rund 20 Standorten folgen. Damit entsteht in der Bundeshauptstadt ein großes 5G Testfeld. »*Wir setzen unseren Weg zur Einführung von 5G in 2020 konsequent weiter fort*«, unterstreicht Claudia Nemat, Vorstand Technologie und Innovation. »*Im Herzen von Berlin machen wir den nächsten Schritt und zeigen, dass nun bereits kommerzielle 5G Technik in unser Netz integriert wird und funktioniert*«.

Aufgebaut wird die kommerzielle 5G Technik vom chinesischen Konzern Huawei. ■

die Informationspflichten nach den Vorschriften der Datenschutzerklärung der DSGVO einhalten. Hier müssen alle Unternehmen, die sich noch nicht um die Datenschutzgrundverordnung gekümmert haben, als erstes aktiv werden. *„Sorgen Sie dafür, dass die Website, überall dort, wo personenbezogene Daten abgefragt werden, SSL-verschlüsselt ist“*, mahnt Floitgraf. Jedes Unternehmen, bei dem sich zehn oder mehr Mitarbeiter mit der Verarbeitung personenbezogener Daten befassen, muss einen Datenschutzbeauftragten haben. Dieser muss schleunigst nicht nur bestimmt werden, sondern auch für Außenstehende leicht erreichbar sein. Daher müssen dessen Kontaktdaten auf der Website vermerkt sein. Eine Adresse wie datenschutz@firma_xy.de gewährleistet beispielsweise, dass ein kurzer Kontaktweg zu ihm zur Verfügung steht.

Gegenüber der Aufsichtsbehörde gilt es, den kompletten Datensatz mit Namen und Anschrift des Datenschutzbeauftragten anzugeben. Ein entsprechendes Meldeformular haben die Aufsichtsbehörden zum 25.5.2018 bereitgestellt. Damit wären den Abmahnanwälten der Zahn gezogen, diese Gefahr ausgeschaltet.

Ebenfalls wichtig ist es, von Anfang an die Mitarbeiter zu sensibilisieren. Denn auch im Vertrieb ändert sich durch die neuen Informationspflichten einiges. Schon beim Erstkontakt muss der Betroffene erfahren, sei er Interessent oder Neukunde, wer seine Daten zu welchem Zweck erfasst und ob sie gegebenenfalls weitergegeben werden. Im Rahmen seiner Betroffenenrechte hat er ein jederzeitiges Auskunfts- und Beschwerderecht gegenüber der Aufsichtsbehörde, wenn er annimmt, dass mit seinen Daten unzureichend umgegangen wird.

Der Datenschutzbeauftragte kommt erneut bei der Dokumentation der Verarbeitungen im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten sowie der technischen und organisatorischen Maßnahmen, mit denen die Daten gesichert werden, ins Spiel. Hier müssen viele Details beachtet werden. Daher sollte diese Aufgabe in Zusammenarbeit mit dem Datenschutzbeauftragten erledigt werden.
Wer bis jetzt noch nichts in Sachen DSGVO getan hat, ist mit den genannten Maßnahmen *„erst einmal aus der vordersten*

René Floitgraf
Geschäftsführer der Spider Network Consulting GmbH, Aachen

Schusslinie raus“ wie es Floitgraf formuliert. Das heißt aber noch lange nicht, dass damit alle Aufgaben erledigt sind und man sich beruhigt zurücklehnen kann.

Als nächstes gilt es nun, die eigenen Dienstleister auf Zulässigkeit zu prüfen. Dazu gehört, dass man eine Vereinbarung zur Auftragsvereinbarung mit den Dienstleistern schließt, sofern diese für das Unternehmen personenbezogene Daten verarbeiten. Wenn das Unternehmen selbst Daten für den Auftraggeber verarbeitet, muss ebenfalls mit dem Auftraggeber eine solche Vereinbarung geschlossen werden. Dafür sollte man vorher seine Dienstleister kennen und wissen welche Daten dort verarbeitet werden. Die Dienstleister müssen im Rahmen der Auftragsdatenverarbeitung gegenüber dem Auftraggeber benannt werden.

Die DSGVO verlangt ausdrücklich, dass Einwilligungen geprüft und verständlich formuliert werden. Sie müssen den Betroffenen unmissverständlich über den Grund der Einwilligung in die Verarbeitung seiner Daten informieren und auch darüber, dass er diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. *„Man muss tunlichst darauf achten, dass das Kopplungsverbot eingehalten wird,*“ so Floitgraf. Der Widerruf darf für den Betroffenen keine negativen Rechtsfolgen, wie das Blockieren des Vertragsabschlusses, haben.

In einem weiteren Schritt muss das Unternehmen die Prozesse im Unternehmen so organisieren, dass Betroffenenrechte berücksichtigt und Datenschutzverstöße in der gesetzlich vorgeschriebenen Zeit gemeldet werden. Wenn im Unternehmen Daten manipuliert oder unrechtmäßig übermittelt wurden oder verloren gegangen sind, muss dies das Unternehmen innerhalb von 72 Stunden bei der Aufsichtsbehörde melden.

Den Betroffenen gegenüber muss das Auskunftsrecht gewahrt werden, sprich er kann jederzeit anfragen, welche Daten über ihn im Unternehmen gespeichert sind. Diese Anfrage muss in maximal vier Wochen bearbeitet sein. Die Auskunft muss vollständig geliefert werden. Dieses Auskunftsrecht ähnelt der kostenfreien Schufa-Anfrage. Dieses Recht steht jedem Betroffenen frei und man kann es nicht einschränken.

Und was hat sich jetzt verändert?

„Der größte Unterschied zum Bundesdatenschutzgesetz liegt in der Rechenschaftspflicht wie sie der Artikel 5 der DSGVO formuliert. Unternehmen müssen nachweisen, dass sie den Datenschutz befolgen. Das gab es in der Form nicht. Man muss ein Bündel an Regelungen und Richtlinien im Unternehmen etablieren und einhalten, um diesen Nachweis zu erbringen“, so Floitgraf. 100 Prozent perfekter Schutz und das Einhalten aller Bestimmungen bis ins Kleinste werden dennoch nicht immer erreicht werden können. Dies liegt daran, dass das Gesetz die Verhältnismäßigkeit im Sinne der Abwägung unterschiedlicher berechtigter Interessen vorsieht. Wenn ein Unternehmen diese Regelung anwendet und die DSGVO eventuell nicht zu hundert Prozent erfüllt, bedeutet das aber noch lange nicht, dass die Aufsichtsbehörde zu der gleichen Einschätzung gelangt. Sie könnte durchaus ein Strafverfahren anstrengen, wobei sich nachvollziehbare Überlegungen des Unternehmens strafmildernd auswirken könnten.

Ebenfalls von großer Bedeutung sind die Informationspflichten, sowohl nach außen hin auf der Unternehmenswebsite als auch gegenüber von einer Datenerhebung Betroffenen. Transparenz und die Kontrolle über die eigenen personenbezogenen Daten wurden deutlich erhöht. Und das EU-weit. Da die EU-DSGVO wie

Industrial Ethernet Switches

Auch wenn's mal rau wird.

Smart City Surveillance

Outdoor Wireless

Factory Automation

DIS-100G Series Industrial Gigabit Unmanaged Switches

Egal, ob in öffentlichen Bereichen oder in der Automatisierungstechnik – unsere Industrial Ethernet Switches haben 5 Jahre Garantie und eignen sich auch für raue Umgebungen. Sie verfügen über einen erweiterten Temperaturbereich, sind Hutschienentauglich und lüfterlos. Mit 30 Jahren Expertise in der Netzwerktechnik wissen wir, wovon wir reden.

PoE-Switche

Für mehr Flexibilität im Netzwerk

PoE Access Points

Für mehr Flexibilität bei der Installation

Sie wollen mehr wissen?
Rufen Sie uns an oder schreiben Sie uns eine E-Mail.
T: **+49 6196 77 99-500** | E: **dce-vertriebsanfrage@dlink.com**
www.dlink.com

D-Link®

jedes große Gesetzeswerk aber dennoch Auslegungsspielräume eröffnet, wird eine wirkliche Rechtssicherheit im Zweifel erst in zwei, drei Jahren eintreten. Dann nämlich werden die ersten Gerichtsverfahren abgeschlossen und klärende Urteile gesprochen sein. Bis dahin sollte man nach bestem Wissen und Gewissen auf Basis der Erfahrungen aus dem Bundesdatenschutzgesetz arbeiten. Und die Bestimmungen der Datenschutzgrundverordnung so gut wie möglich einhalten. Damit ist Unternehmen und ihren Kunden am meisten gedient. *„Die DSGVO stellt niemanden vor unlösbare Herausforderungen. Sie gibt dem Datenschutz und der Wahrung der Privatsphäre einen großen Schub. Und das ist heute wichtiger denn je“*, resümiert Floitgraf. ■

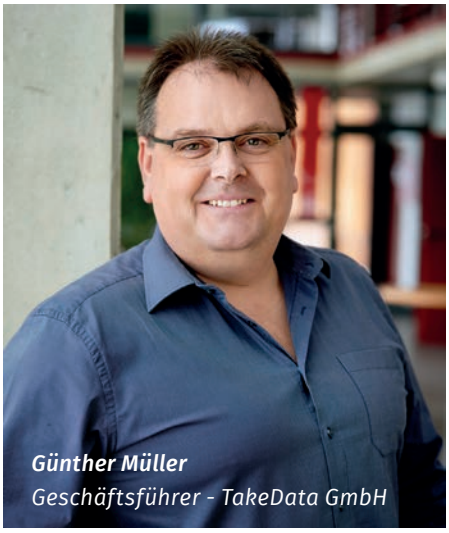
Industrie 4.0

Neue Lösungen gegen neue Bedrohungen durch IoT

In vielen Haushalten sind Internet-of-Things-Geräte plötzlich Alltag, auch in der Industrie halten sie allmählich Einzug. Doch an Sicherheit wird dabei kaum gedacht. Firewalls und Security-Lösungen können nur bedingt etwas dagegen ausrichten.

© 331223288 – shutterstock

Die gute Nachricht: 100 Prozent der deutschen Unternehmen mit zehn oder mehr Mitarbeitern schützen ihre Daten und Netze mit Passwörtern, Firewalls, Virenscannern und durch das Anlegen von Backups. Das hat eine repräsentative Umfrage des IT-Branchenverbands Bitkom im vergangenen Jahr ergeben. Doch bei diesen einfachen Maßnahmen bleibt es häufig auch. Beispielsweise Intrusion-Detection-Systeme setzt nur jedes fünfte Unternehmen ein. Und obwohl der Faktor Mensch immer wieder als Schwachpunkt in der IT-Sicherheit genannt wird, geben nur 53 Prozent der Unternehmen an, auf Mitarbeiterschulungen zu setzen, um ihre digitale Infrastruktur und ihr Know-how zu schützen.


Günther Müller
Geschäftsführer - TakeData GmbH

TakeData-Systems GmbH

Insofern ist es nicht überraschend, dass mehr als 50 Prozent der Unternehmen angeben, in den vergangenen zwei Jahren von Datendiebstahl, Spionage oder Sabotage betroffen gewesen zu sein. Weitere 26 Prozent vermuten, dass sie betroffen gewesen sind. Trotzdem scheint der Handlungsdruck gering zu sein. *„Wir haben keine Zeit dafür. Irgendwann müssen wir mal was machen.“* Diese und auch ähnlich lautende Reaktionen hat die TakeData-Systems GmbH aus Straubing erhalten. *„Wir hatten noch nie Probleme, daher lassen wir lieber alles, wie es ist“*, war eine weitere Rückmeldung.

IoT-Hersteller gehen eigene Wege

Günther Müller ist vom genauen Gegenteil überzeugt. Der TakeData-Geschäftsführer betrachtet IT-Sicherheit nicht als etwas Starres, das man besser nicht mehr anfasst, sobald es einmal erfolgreich eingerichtet ist, sondern als einen dynamischen Prozess, der sich ständig neuen Herausforderungen anpassen muss. *„Viele arbeiten mit statischen Lösungen, mit Black- und Whitelists,“* wundert er sich, *„statt beispielsweise permanent zu überwachen ob eine bestimmte Website sauber ist oder nicht.“* TakeData setzt dafür auf Forcepoint, eine Sicherheits-Suite, die unter anderem URL-Sandboxing ermöglicht. *„Wenn Sie eine E-Mail mit*

einem Link bekommen, wird der Link durch einen temporären Link ersetzt", erklärt Müller. Dieser Link führt zum Forcepoint-System, das dann die eigentliche Adresse aufruft und deren Inhalte auf Unschädlichkeit prüft – ein Beispiel dafür, wie dynamische, sich an Bedrohungen anpassende IT-Sicherheit funktionieren kann. So kann der Sicherheitsmechanismus unmittelbar aktiv werden, sobald sich die Inhalte einer Website verändern. Mit gewisser Sorge betrachtet Günther Müller den Einzug von vernetzten Sensoren und Maschinen in mittelständische Unternehmen. Denn das kann die IT-Sicherheit massiv aushöhlen und ein Einfallstor für Hacker und Trojaner sein. Denn die Hersteller arbeiten bei der Übertragung der IoT-Daten mit verschiedensten Protokollen wie HTTP, CoAP, XMPP und MQTT. Die Schwierigkeit liegt in der Integration in die Security-Lösung der Unternehmen, ohne dass Löcher entstehen und IoT-Geräte unkoordiniert und unkontrolliert ungewollte Datenverbindungen mit internen und externen Geräten aufbauen können. Zwar kenne er noch kein Beispiel von einem Kunden, bei dem das Internet of Things (IoT) zum Sicherheitsproblem wurde, aber das liege wohl daran, dass die Integration der Technik in Anlagen noch nicht weit fortgeschritten sei. „*Das geht in der Industrie langsamer als bei Consumer-Technik*", sagt Müller. „*Aber jeder probiert es aus.*"

Anomalien aufspüren behebt Ursachen nicht

Eine leistungsstarke Security-Lösung kann das Schlimmste verhindern. „*Wir können sehen, wenn es Anomalien im Netz gibt*", sagt Müller. „*Wenn normalerweise 50-70 Geräte ins Internet wollen und plötzlich sind es 200, kann Forcepoint Alarm schlagen.*" Dieses Szenario beschreibt eine DDoS-Attacke, für die IoT-Geräte schon mehrfach missbraucht wurden. Ein Trojaner schlummert auf den Sensoren, bis Tausende von ihnen plötzlich gleichzeitig einen bestimmten Server kontaktieren und dadurch lahmlegen. „*Aber wir können nur die Auswirkungen abfangen, das eigentliche Problem müssen die Hersteller der IoT-Geräte lösen*", so Müller.

Um sinnvoll etwas gegen Angriffe ausrichten zu können, hält der TakeData-Geschäftsführer zudem die weit verbreiteten UTM-Firewalls für unzureichend. Müller plädiert dafür Firewall und Web-Security zu trennen. Während sich die Firewall auf ihrer eigenen Hardware darum kümmert, das Unternehmensnetz abzusichern, VPN-Zugänge zu managen oder auch die Quality of Service bei der Internettelefonie sicherzustellen, sorgt ein eigener Server für Sicherheit beim Datenaustausch via Web und E-Mail. Damit das flüssig gelingt, brauche es bei 200 bis 300 Nutzern schon vier bis sechs Prozessoren und 32 oder 64 Gigabyte Arbeitsspeicher – weitaus mehr als in der handelsüblichen UTM-Firewall stecke. Ein solches System könne „on Premise" installiert werden oder remote in der Cloud laufen. Es helfe auch dabei, den Anforderungen der neuen Datenschutzgrundverordnung gerecht zu werden. „*Unternehmen müssen einen Datenverlust innerhalb von 72 Stunden melden*", erklärt Günther Müller. „*Unser Reporting-System loggt mit, wann welche Daten wohin gesendet wurden.*"

Doch Müller will nicht um jeden Preis in jedem Unternehmen ein solches System installieren. Er plädiert nur dafür, IT-Sicherheit nicht auf die lange Bank zu schieben. „*Es gibt eine Augen-zu-und-durch-Mentalität*", kritisiert er und will Unternehmen die Augen öffnen: „*Es ist super, wenn mir meine Anlage übermittelt, dass die Kurbelwelle bald eine Reparatur benötigt, aber muss das über die Cloud geschehen?*" Sensoren, die Maschinen überwachen, gebe es schon lange, der Mehrwert einer Internetanbindung sei nicht immer gegeben. Aber wenn man diesen Schritt gehen wolle, dann müsse man „*den ersten Schritt vor dem zweiten tun*", so Müller, und sich vorab um die IT-Sicherheit kümmern. Sonst könnte der Schaden, den Datendiebstahl, Industriespionage und Sabotage in Deutschland anrichtet, in Zukunft stark steigen. In den vergangenen zwei Jahren lag er laut der Bitkom-Befragung schon bei fast 110 Milliarden Euro. ■

VR-Headsets

Warum sich Unternehmen für Virtual Reality interessieren sollten

Die Virtual-Reality-Technik sorgte lange Zeit für Euphorie in der Gaming-Szene. Dabei liegen die interessantesten Anwendungsfelder woanders: **im Geschäftsbereich.**

© 498623428 – shutterstock

Nicht immer sind die vielen praktischen Anwendungen einer neuen Technik direkt ersichtlich. Als 2007 das erste iPhone auf den Markt kam, war das erstmal nur ein Touchscreen-Handy – und niemand ahnte, wie viele Apps es dafür einmal geben würde, die wir heute täglich nutzen.

Mit der Virtual Reality (VR) ist es in gewisser Weise ähnlich. Die Technik an sich ist nicht sonderlich spektakulär ohne Anwendungen, die sich Unternehmen, Spiele- und Medienentwickler dafür ausdenken. Der Anwender trägt hierbei ein Headset (auch VR-Brille genannt). Jedes Auge erhält durch ein eigenes Display ein individuell erzeugtes Bild, das sorgt für den stereoskopischen 3D-Effekt. Verbaute Kopfhörer versorgen die Anwender zusätzlich mit Umgebungsgeräuschen – ebenfalls immer an die jeweilige Situation und Blickrichtung des Anwenders angepasst. Das VR-Headset soll so eine möglichst detailgetreue Simulation einer real gefilmten oder frei generierten Umgebung erzeugen. Der Anwender taucht komplett in sie ein (Immersion genannt), von seiner echten Umgebung bekommt er abgesehen von Umgebungstemperatur und Geruch nichts mehr mit – wobei sogar schon getestet wurde, auch den Geruch zu simulieren.

Viele Jahre galt die VR-Technik als eine, die die Gaming-Branche revolutionieren könnte. Doch die Hürden für Privatanwender sind recht groß: Sie zahlen ein paar hundert Euro für ein VR-Headset, wie HTC Vive oder Oculus Rift, und müssen zudem noch einen leistungsfähigen Rechner bereitstellen, der das Headset mit Inhalten versorgt. Auch deshalb haben sich die VR-Headsets im privaten Bereich noch nicht durchgesetzt.

Vom Architekten bis zum Industrie-Konzern

Im Business-Bereich sieht das anders aus. *„Die Unternehmen haben die VR-Technik auf dem Schirm“*, sagt Tom Neubert, Produktmanager Virtual und Augmented Reality bei der Schenker Technologies GmbH in Leipzig. Das Unternehmen produziert hochwertige Business- und Gaming-Rechner und vertreibt seit einigen Jahren auch VR-Technik. *„Fast alle unsere VR-Kunden sind Unternehmen“*, sagt Tom Neubert – und das sei nicht verwunderlich. Denn zum einen spielten für sie die Anschaffungskosten für die Hardware eine nicht so große Rolle, zum anderen gebe es viele Anwendungsfelder, in denen Virtual Reality den Unternehmen einen großen Nutzen bringen kann. **Das sind zum Beispiel:**

- Ein Architekturbüro erstellt am Rechner ein 3D-Modell des geplanten Hauses. Je nachdem, welche CAD-Software benutzt wird, ist bereits eine Schnittstelle zur Virtual-Reality-Software vorhanden. Mit ihr können sich Architekt und Kunden das geplante Haus in einer virtuellen Realität angucken und ein nahezu echtes Gefühl dafür bekommen, wie die Räume später wirken werden. Wird die eigentliche VR-Technik erweitert durch eine Positionsbestimmung, kann der Anwender, der die VR-Brille trägt, sogar durch einen (echten) Raum gehen – die Software berücksichtigt die Position und passt die virtuelle Umgebung darauf an. So wirkt das Erlebnis in der virtuellen Realität noch realistischer. Tom Neubert von Schenker Technologies schätzt den Aufwand eines solchen Angebots prinzipiell als nicht zu hoch ein: „Wer Lust hat, sich damit zu beschäftigen, bekommt das hin.“ Für die Hardware fallen circa 2000 Euro an: 450 bis 800 Euro für die VR-Brille, 1500 für den leistungsfähigen Rechner, der im Falle eines Architekturbüros vielleicht sogar schon vorhanden ist.

- Ein Unternehmen hat ein neues Produkt entwickelt, zum Beispiel ein Fahrrad, Auto oder einen Kaffee-Vollautomaten. Nun wollen die Verantwortlichen das Look-and-Feel des Produktes so realistisch wie möglich erleben, ohne einen Prototypen bauen zu müssen. Mehrere Mitarbeiter verabreden sich zu einem Virtual-Reality-Meeting und schauen sich gemeinsam das neue Produkt an. Möglich ist es für sie auch, das neue Produkt zu bedienen, wenn das vorher so programmiert wurde. Durch die Interaktion mit Hilfe eines intuitiven

Controllers könnte also beim Auto die Tür aufgehen, wenn der Anwender in der virtuellen Realität an der richtigen Stelle steht und seine Hand zur Autotür bewegt.

• Ein Hersteller von Industriemaschinen will seinen Servicemitarbeitern, die auf der ganzen Welt verteilt sind, zeigen, wie die Maschinen gewartet werden. Der Trainer organisiert eine Schulung, bei der alle Servicekräfte ein Virtual-Reality-Headset tragen und über das Internet miteinander verbunden sind. So können alle gleichzeitig in der virtuellen Realität live an der Maschine sehen, wie sie gewartet werden muss, ohne dass ein einziger Mitarbeiter tatsächlich in der Nähe einer echten Maschine sein müsste.

Die Beispiele zeigen: Die Virtual-Reality-Technik kann 3D-Welten simulieren und vielen Menschen an unterschiedlichen Orten erlebbar machen. Dabei spielt es keine Rolle, ob es die dargestellte Welt wirklich gibt (bereits gebaute Industriemaschinen) und sie nur deshalb ins Virtuelle übertragen wird, weil sie so für viele Menschen verfügbar wird – oder ob das Gezeigte eben rein virtuell ist und zum Beispiel einen noch nicht gefertigten Prototypen darstellt.

„Seit die VR-Technik ausgereift und gut zu bedienen ist, gibt es immer mehr Use Cases, die zeigen, wo die Technik Unternehmen einen Mehrwert bieten kann“, sagt Tom Neubert. Und das wissen inzwischen auch viele Unternehmen. Er besuche regelmäßig Veranstaltungen, wo Unternehmen fragen, ob Virtual Reality für einen bestimmten Einsatzzweck denkbar ist oder wo sie bei ihnen Anwendung finden könnte.

Wie groß der Aufwand für ein Unternehmen ist, Virtual-Reality-Projekte umzusetzen, ist sehr unterschiedlich. Manchmal müssen nur ein paar hundert Euro und einige Stunden Zeit investiert werden. Will jedoch zum Beispiel ein Autobauer interessierten Kunden ein neues Automodell emotional vermitteln und die VR-Technik zu Marketingzwecken nutzen, sind die Ansprüche an VR-Konzept, Bildqualität und Sounddesign höher. Hinzu kommt: Bei der VR-Technik müssen die Bilder in Echtzeit gerendert werden. Ist der Anspruch an die Qualität sehr hoch, braucht es entsprechend leistungsfähige und teure Hardware. Auch kann ein Unternehmen ein solches Projekt vielleicht nicht mehr selbst umsetzen und braucht Unterstützung von einem spezialisierten 3D-Studio.

AR: Nicht nur virtuell

Verwandt mit der Virtual-Reality-Technik ist die der Augmented Reality (AR), was für erweiterte Realität steht. Auch hier trägt der Anwender eine Art Brille, allerdings lässt diese ihn seine echte Umgebung weiterhin wahrnehmen. Die Umgebung wird durch entsprechende Projektionstechniken in der Brille mit virtuellen Inhalten erweitert. Auch hierfür gibt es schon Beispiele aus der Praxis: Soll ein Techniker eine Maschine reparieren, und gehört diese Aufgabe nicht zu seinem Arbeitsalltag, kann er von einer Augmented Reality unterstützt werden. Bei der Reparatur trägt er ein AR-Headset, und dieses zeigt beispielsweise in seinem Sichtfeld an, welches Bauteil welches ist und in welcher Reihenfolge sie zu demontieren sind.

Die AR-Technik ist hauptsächlich durch die AR-Brille „Google Glass“ bekannt geworden, die ab 2014 im Verkauf war – allerdings nicht lange. Google war mit dem Verkaufsergebnis nicht zufrieden, und es kamen Bedenken in der Öffentlichkeit auf, dass die Träger der Brille jederzeit alle Menschen in der Umgebung filmen könnten, ohne dass diese das mitbekommen. *„Bis heute ist die technische Vielfalt bei der AR-Hardware noch nicht so groß“*, sagt Tom Neubert von Schenker Technologies. Aber auch hier tut sich was: Die Technik wird besser, und auch für die Augmented Reality werden Unternehmen spannende und nützliche Anwendungen finden. ■

© Andrey Popov - #165900130 - Fotolia.com

Gesundheit

Fitness-Übungen fürs Büro, die niemand bemerkt

Keine Zeit ins Fitness-Studio zu gehen? Keine Lust auf Sport? Kleine Verhaltensänderungen und unauffällige Übungen können den Büro-Alltag nebenbei zum Workout machen.

Dass der Körper fit sein muss, damit auch der Geist gut arbeitet, ist kein Geheimnis. Und genauso gehört es wohl zum Allgemeinwissen, dass Stehen oder Gehen besser ist als Sitzen, Treppensteigen gesünder als Aufzugfahren. Aber der Mensch ist bequem, und wer will es ihm verübeln? Wer trotzdem Lust hat: Die folgenden einfachen Übungen können nicht nur den Körper stärken, sondern bringen auch etwas Abwechslung in den Büroalltag ohne allzu auffällig zu sein und die Blicke der Kolleginnen und Kollegen anzuziehen:

Die einfachste Art, die Zeit im Büro auch für den Körper sinnvoll zu nutzen, sind kleine Verhaltensänderungen. Statt für kurze Absprachen zum Telefon zu greifen oder eine E-Mail zu schreiben, besuchen Sie die Kollegin oder den Kollegen an ihrem oder seinem Schreibtisch. Halten Sie vermehrt Besprechungen im Stehen ab. Das bringt nicht nur mehr Dynamik in Körper und Geist, sondern verkürzt auch die Dauer von Besprechungen – schließlich möchten wir dann doch wieder zurück in den bequemen Schreibtischstuhl.

Schreibtisch anheben

Aber auch im Sitzen kann man etwas für den Körper tun. Ob in einem Meeting oder am Schreibtisch: Sie können beispielsweise versuchen, den Tisch von unten mit den Handflächen anzuheben – stellen Sie nur sicher, dass der Tisch schwer genug ist, sodass Sie ihn nicht tatsächlich anheben! Drücken Sie gegen die Tischplatte, bis Ihre Muskeln ermüdet sind. Dann legen Sie Ihre Hände auf den Tisch und versuchen, ihn in den Boden zu drücken, ebenfalls bis Sie keine Kraft mehr haben. Ob Sie diese Übungen mit beiden Händen gleichzeitig oder abwechselnd machen, bleibt Ihnen überlassen. Für Extra-Fleißpunkte können Sie beim Herunterdrücken auch noch-gleichzeitig die Beine ausstrecken und so hoch heben wie möglich. Das dürfte Ihnen auch eine Pose verleihen, die Sie sehr aufmerksam aussehen lässt.

Übung am Kopierer

Etwas auffälliger sind Übungen im Stehen. Aber sie lassen sich dennoch gut in den Büroalltag integrieren – etwa wenn Sie dabei telefonieren oder am Kopierer warten müssen. Stützen Sie sich mit einer oder beiden Händen auf der Rückenlehne Ihres Stuhls oder am Kopierer ab. Die Füße schulterbreit auseinander, verlagern Sie Ihr Gewicht auf ein Bein und heben das andere Bein leicht nach hinten ausgestreckt an. Machen Sie kleine kreisende Bewegungen mit dem Bein: circa 25 Mal im Uhrzeigersinn, dann 25 Mal gegen den Uhrzeigersinn. Wiederholen Sie das Ganze mit dem anderen Bein.

Wenn Sie eher ein klassisches Krafttraining bevorzugen, werden Sie kreativ. Nutzen Sie Wasserflaschen anstelle von Hanteln. Stützen Sie sich am Schreibtisch ab, um Liegestützen nicht auf dem Boden machen zu müssen. Und wer das Ganze professionalisieren will: Überzeugen Sie Ihren Chef, Fitness und Sport als Angebot für alle einzurichten.

Die universellste Übung fürs Büro: mehr Lachen. Das stärkt die Bauchmuskeln, ist gut fürs Herz und baut Stress ab. ■

© WrightStudio - #162595784 - Fotolia.com

Schlüssel zu mehr Sicherheit

Die Einführung von Multifaktor-Authentifizierung kann wesentlich dazu beitragen, die Sicherheit im Unternehmen zu verbessern. Der Zugang ungebetener Besucher, die Sicherung der IT und die korrekte Erfassung von Arbeitszeiten lassen sich auf diese Weise einheitlich lösen.

Bei mittelständischen Unternehmen, Behörden und Praxen, wo einerseits sensible Daten gespeichert werden und andererseits regelmäßig Besucherverkehr vorhanden ist, sollten besondere Vorsichtsmaßnahmen beherzigt werden. Denn gerade dort, wo regelmäßig Besucher ein- und ausgehen, muss mit Angriffsversuchen von Cyberkriminellen oder Betriebsspionen gerechnet werden. Es wäre leider nicht das erste Mal, dass ein vermeintlicher Paketbote oder Servicetechniker ein Spionagetool ins Firmennetzwerk schleust. Auch eine Arztpraxis kann zum Ort cyberkrimineller Vergehen werden: Etwa dann, wenn sich Patienten Rezepte selbst ausdrucken wollen, oder der eifersüchtige Ehemann prüfen will, ob seine Frau wirklich am Vortag beim Arzt war. Oft ist es ein Leichtes, sich in einer unbeobachteten Minute Zugang zum Praxisinformationssystem zu verschaffen.

In beiden geschilderten Fällen kann der „erfolgreiche“ Missbrauch zu erheblichen Problemen führen. Landen sensible Firmendaten bei der Konkurrenz, kann das jahrelange Entwicklungsarbeit zunichte machen. Gelangen sensible Patientendaten unbemerkt in falsche Hände, drohen womöglich Ermittlungen wegen Datenmissbrauchs. Die oft mühevoll aufgebaute Reputation des Unternehmens oder der Praxis leidet dann empfindlich. Vermeiden lassen sich solche Rückschläge mit Lösungen zur Multifaktor-Authentifizierung.

© 764978650 - shutterstock

Alternative zu Biometrie

Klingt kompliziert, ist es aber nicht. Marktführender Anbieter solcher Lösungen ist das in Furtwangen ansässige Unternehmen Reiner SCT. Der Grundgedanke solcher Lösungen ist es, dass sich Mitarbeiter stets über zwei Wege identifizieren müssen. Auf diese Weise ist es für eine unbefugte Person quasi unmöglich, sich in einen PC einzuloggen: Für den Zugang genügt es, die Chipkarte ins Lesegerät zu stecken. Wird sie aus dem Gerät gezogen, wechselt Windows automatisch zum Sperrbildschirm. Im Gegensatz zum einfachen Passwort

oder Zugangscode bietet die von Reiner SCT angebotene Lösung Secure Logon 2 ein deutlich höheres Sicherheitsniveau. Auch biometrischen Erkennungsverfahren wie Gesichtserkennung oder Fingerabdruck ist die Chipkarte wegen der höheren Erkennungsgenauigkeit überlegen.

„Gerade im Hinblick auf die EU-Datenschutzgrundverordnung (DSGVO) sollten viele Unternehmen und Praxen noch einmal kritisch prüfen, ob sie wirklich ausreichend geschützt sind“, gibt Vertriebsleiter Peter Thomas zu bedenken. *„Noch immer ist es in vielen Unternehmen Gang und Gebe, dass PC in nur mit einem simplen Passwort wie ‚12345‘ oder ‚passwort‘ geschützt sind. Im Zweifelsfall findet ein Hacker den Zugangscode, indem er ganz einfach einmal unter die PC-Tastatur oder die Schreibtischunterlage schaut“*, warnt Thomas. Spätestens mit dem Inkrafttreten der neuen DSGVO-Regelungen sollten Unternehmen hier nachbessern, denn wenn grundlegende Sicherheitsvorkehrungen quasi nicht vorhanden sind, können den Betroffenen schnell empfindliche Strafen drohen.

Reiner SCT-Vertriebsleiter Peter Thomas: „Im Hinblick auf die DSGVO die vorhandenen Schutzmaßnahmen kritisch prüfen.“

Schrittweiser Ausbau

Der Ausbau der Sicherheit am PC kann dabei als „Grundstein“ zu einer insgesamt nachhaltigen Absicherung dienen: Reiner SCT bietet nicht nur Chipkartenleser für den PC an, sondern auch Komplettlösungen, die schon am Hauseingang ansetzen. Mit diesen Lösungen können sich Mitarbeiter bereits an der Büropforte bequem authentifizieren, optional werden im gleichen Schritt Arbeitsbeginn und Arbeitsende erfasst. Unternehmen können auf diese Weise auch steuern, welche Mitarbeiter für welche Räumlichkeiten eine Zutrittsberechtigung erhalten. Kann ein Mitarbeiter bestimmte Bereiche – etwa die Entwicklungsabteilung – erst gar nicht betreten, sinkt automatisch das Missbrauchsrisiko. Vorteilhaft für die Nutzer: Der Angestellte braucht sich nur einen einfachen PIN-Code zu merken. Das komplexe Passwort ist verschlüsselt auf der Chipkarte vermerkt.

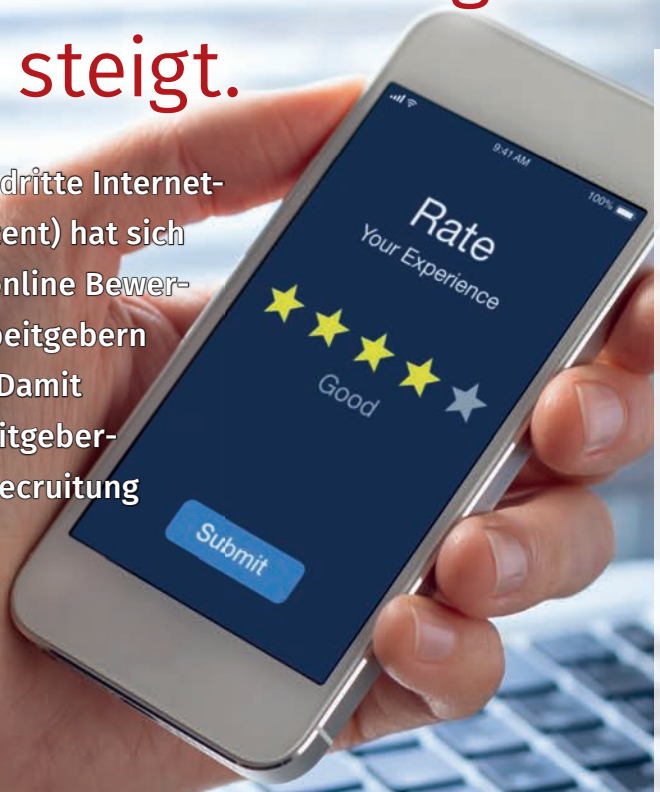
Reiner SCT bietet die Lösungen zur Multifaktor-Authentifizierung in einer Art Baukasten-System an. Ein Unternehmen kann somit beispielsweise zuerst die PC schützen und das System später auf den Schutz des Eingangsbereichs oder um die Zeiterfassung erweitern. ■

Weitere Infos zum Thema:
Reiner SCT, Thomas Peter, Tel.: +49 (7723) 5056-700, E-Mail: tpeter@reiner-sct.com, www.reiner-sct.com

Recruiting

Interesse an Arbeitgeber-Bewertungen online steigt.

Mehr als jeder dritte Internetnutzer (36 Prozent) hat sich schon einmal online Bewertungen von Arbeitgebern durchgelesen. Damit gewinnen Arbeitgeberportale beim Recruitung an Bedeutung.



© NicoElNino - #179843886 - Fotolia.com

Seit 2015 ist die Zahl derjenigen, die sich auf entsprechenden Online-Plattformen informieren, um sieben Prozentpunkte gestiegen, hat eine repräsentative Umfrage des Branchenverbands Bitkom ergeben.

„Ob zur groben Orientierung oder zur Überprüfung nach einem ersten Kontakt: Online-Rezensionen spielen in der Arbeitswelt genauso wie in anderen Bereichen – etwa bei Produkten, Hotels oder Dienstleistungen – eine immer größere Rolle“, sagt Juliane Petrich von Bitkom. Arbeitgeber sollten die Bewertungen daher ernst nehmen. Auch ob ein Arbeitgeber auf eine Online-Bewertung reagiere und wie er reagiere, könne zum Image der Firma beitragen, so Petrich. *„Für viele Berufstätige sind Online-Bewertungen die erste Visitenkarte eines Arbeitgebers.“*

Arbeitgeberbewertungen werden jedoch nicht nur gelesen, sondern auch immer öfter selbst verfasst. Dem eigenen Arbeitgeber hat jeder vierte Befragte schon einmal online eine Bewertung hinterlassen. ■

WORTMANN AG empfiehlt Windows 10 Pro.

TERRA PAD 1270

terra
IT. MADE IN GERMANY.

Hervorragend ausgestattetes Business-Tablet mit zahlreichen Anschlüssen und bis zu 9 Stunden Akkulaufzeit.

TERRA PAD 1270
mit Type Cover, Stylus und LTE

- Intel® Core™ i5-7Y54 Prozessor (4M Cache, bis zu 3.20 GHz)
- Windows 10 Pro
- 30.48 cm (12") Touch Display, 2160x1440 Pixel Auflösung
- 8 GB RAM, 256 GB SSD
- Card Reader Micro SD
- LTE, GPS, WLAN, Bluetooth

Artikel-Nr.: 1220561

beleuchtete Tastatur

1299,-* inkl. gesetzl. MwSt.

Optional:

PAD 1270 Erweiterungsmodul

Erweitert das PAD um einen USB 3.0 und einen HDMI Anschluss + mehr Akkuleistung

Artikel-Nr.: 1480071

199,-* inkl. gesetzl. MwSt.

Optional:

PAD 1270 Dockingstation

3x USB 3.0, 1x USB 3,0 Typ C, 1x HDMI
1x Display Port, 1x LAN

Artikel-Nr.: 1480076

149,-* inkl. gesetzl. MwSt.

Nur über Systemhäuser erhältlich. Jetzt Händler finden: www.wortmann.de/partner

*Aktionspreis inklusive Mwst. Bei teilnehmenden Händlern erhältlich. Angebot gültig solange der Vorrat reicht. Keine Mitnahmegarantie. Änderungen und Irrtümer vorbehalten. Solange der Vorrat reicht.

Ultrabook, Celeron, Celeron Inside, Core Inside, Intel, das Intel-Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, das „Intel Inside"-Logo, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, vPro Inside, Xeon, Xeon Phi, Xeon Inside und Intel Optane sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

WORTMANN AG
IT. MADE IN GERMANY.

© 710886218926 – shutterstock

Wir digitalisieren Zukunft

comTeam Technologie-Partner sind Ihre Spezialisten für IT- und TK-Projekte – regional und bundesweit.

Als Partner im comTeam Technologie-Netzwerk greifen wir auf ein bundesweites Service-Netzwerk mit 10.000 IT-Spezialisten zurück, um Ihre Anforderungen zu verstehen, Lösungen zu erarbeiten und Ihr Unternehmen erfolgreich in die digitale Zukunft zu führen.

www.comteam-marketplace.de

WIR DIGITALISIEREN ZUKUNFT

comTeam DAS TECHNOLOGIE-NETZWERK