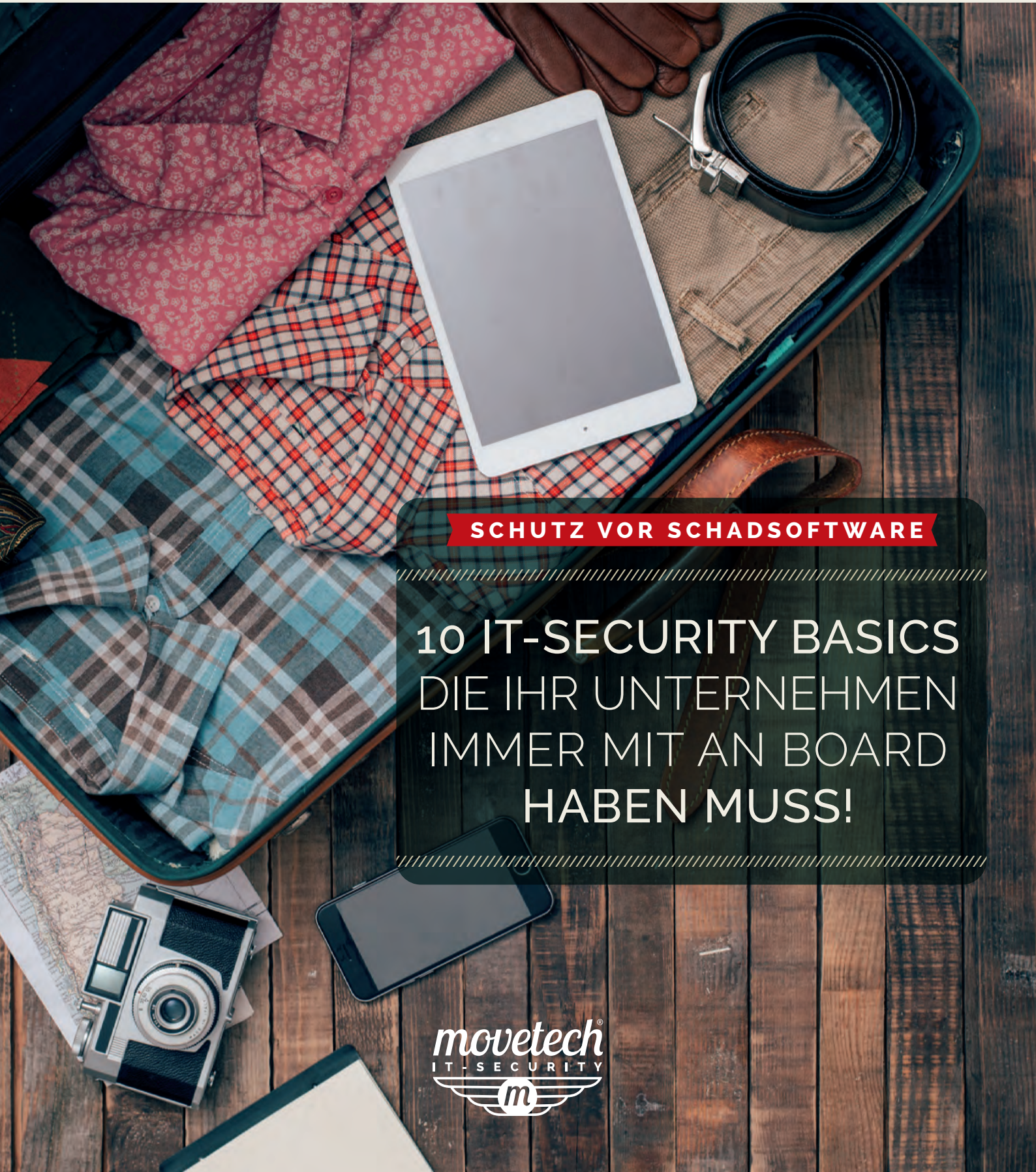
EXCLUSIVE

IT-Security-Magazine

EDITION NO2



SCHUTZ VOR SCHADSOFTWARE

10 IT-SECURITY BASICS DIE IHR UNTERNEHMEN IMMER MIT AN BOARD HABEN MUSS!

movetech® IT-SECURITY

10 IT-Security Basics, die Sie umsetzen müssen

AUS AKTUELLEM ANLASS:

Nachdem die Schadsoftware Emotet unter anderem die Uni Gießen, diverse Behörden und Unternehmen in Hessen teils lahmgelegt hat, möchten wir Sie auf Maßnahmen aufmerksam machen, mit denen Ihre IT-Umgebung dagegen geschützt werden kann.

In vielen Unternehmen hinkt die IT-Sicherheit dem Stand der Technik hinterher. Auch werden häufig Sicherheitslösungen angeschafft, ohne dass deren Wirksamkeit überprüft wird. Die interne oder externe IT muss kaum kritische Fragen der Geschäftsführung fürchten. Das möchten wir hiermit ändern. Deshalb haben wir 10 Basics zusammengestellt, die aktuell definitiv in Ihrem Unternehmen implementiert sein müssen. Ja, das ist technisch und anspruchsvoll, aber: **Die IT-Sicherheit sollte auch in Ihrem Unternehmen Chef*innen-Sache sein** – fragen Sie nach, ob und wie diese Basics bei Ihnen umgesetzt werden.

1. Backups

Wie oft werden die Backups erstellt? Wieviele Tage „können" Sie nachweislich zurück? Wird regelmäßig überprüft, ob sich Daten aus Backups zuverlässig wiederherstellen lassen? Gibt es Offline-Backups? Gehen Sie nach der 3-2-1-Regel vor?

2. Firewall

Besitzt Ihr Unternehmen eine professionelle UTM-Firewall? Gibt es echte Regel- oder Filtersets oder lautet die Regel einfach nur „any out"? Werden die Geräte überwacht? Wer kümmert sich regelmäßig und nachweisbar um die Updates der Firmware?

3. Antivirus-Lösung

Haben Sie eine professionelle Antivirus-Lösung auf Ihren Servern und Endgeräten installiert, die sich zentral verwalten lässt? Werden die Meldungen der Software täglich oder öfter ausgewertet?

4. Passwörter / 2-Faktor-Authentisierung

Werden die Kennwörter in einem Passwordsafe (z.B. Keepass, Passwordstate) gesichert? Existiert in Ihrem Unternehmen eine Kennwortrichtlinie? Gibt es eine 2-Faktor-Authentisierung bei möglichst vielen wichtigen Diensten und Anwendungen? Haben Sie als Geschäftsführer zumindest theoretisch Zugriff auf mindestens ein Domain Administrator Passwort?

5. Updates / Monitoring

Werden die Updates der Betriebsysteme & Software Ihrer PCs/Server zentral ausgerollt und der Patchstand regelmäßig überwacht? Wird die Firmware Ihrer Switches, Drucker, Router, WLAN-Umgebung etc. nachweisbar regelmäßig aktualisiert? Werden die aktiven Komponenten in Ihrem Netzwerk dauerhaft auf Fehler überwacht? Haben Sie Zugriff auf eine Gesamtübersicht?

6. Netzwerk-Segmentierung

Wird bei Ihnen die Netzwerk-Segmentierung konsequent umgesetzt? Das bedeutet zum Beispiel: Sind Office-IT und Produktions-IT voneinander getrennt? Hat die Produktions-IT dauerhafte Schnittstellen in andere, mit dem Internet verbundene, Netze? Ist Sie gar direkt mit dem Internet verbunden? Sind Ihre PCs, Server, Telefone, Drucker und vor allem die Managementschnittstellen aller Geräte in eigene Netze separiert?

7. Schulungen

Werden Ihre Mitarbeiter regelmäßig für die Gefahren sensibilisiert, die durch E-Mail-anhänge oder Office Makros in entstehen können? Wissen Ihre Mitarbeiter, an wen sie sich bei Auffälligkeiten wenden sollten?

8. Dokumentation

Haben Sie Zugriff auf eine ausführliche und vor allem aktuelle Dokumentation Ihrer IT-Umgebung? Dazu gehört auch eine Auflistung aller Softwarelizenzen, Laufzeiten von Serviceverträgen und Carepacks, eine Übersicht des Netzwerks und der VLAN-Konfiguration auf den Switches etc. Gibt es davon auch eine physische Kopie außerhalb des Gebäudes?

9. Administratorrechte

Gibt es Benutzer, die mit lokalen Administrator-rechten arbeiten? Haben diese Benutzer direkten Zugriff auf das Internet? Wird ver-mieden, dass zu Supportzwecken ein Benutzer mit Domainadminrechten auf die PCs der Benutzer zugreift? Ist in ihrem Netzwerk eine strikte Rechtetrennung im LDAP bzw. Active-Directory (3-Tier-Modell) implementiert?

10. Externe Festplatten / USB-Sticks / Verschlüsselung

Sind USB-Sticks und externe Festplatten bei Ihnen grundsätzlich verboten oder funktionieren nur bestimmte ausgewählte Geräte? Sind die Speicher aller mobilen Geräte, Sticks und Festplatten grundsätzlich immer verschlüsselt? Das ist vor dem Hintergrund der Meldepflicht der DSGVO bsonders wichtig!

Wenn Sie diese Punkte beachten und implementiert haben, sollte das Sicherheitsniveau Ihrer IT schon verhältnismäßig hoch sein.

Haben Sie zusätzlich im Blick, dass es sich bei der IT-Sicherheit nicht lediglich um eine einmalige Anschaf-fung, sondern um einen fortlaufenden Prozess handelt, befinden Sie sich mit Ihrem Unternehmen auf dem richtigen Weg zu mehr Sicherheit.

Sofern Sie viele Antworten wie „Brauchen wir nicht.“, „Ist übertrieben.“ oder „Viel zu teuer.“ erhalten, ist Ihr Unternehmen aktuell möglicherweise anfällig für eine Attacke und sollte höchstwahrscheinlich im Bereich IT-Sicherheit nachbessern.

Ein Blick auf die aktuell betroffenen Netzwerke lohnt sich: Rechnen Sie einmal aus, was es Ihr Unternehmen insgesamt kosten würde, wenn die gesamte IT für nur 1-2 Wochen gar nicht mehr vorhanden wäre, nichts mehr funktionierte und wirklich alles schlimmstenfalls komplett von Grund auf neu installiert werden müsste. Das Ergebnis dürfte in den allermeisten Fällen die obi-gen Antworten als falsch entlarven.

Falls Sie noch Fragen zu dem Thema haben, sprechen Sie uns gerne an oder besuchen Sie eine unserer exklusiven Veranstaltungen. Dort gehen wir verständlich und anschaulich auf das Thema IT-Sicherheit aus Sicht der Geschäftsführung ein.

Buchen Sie Ihr Ticket für unsere exklusiven Unternehmerabende!

Lernen Sie uns bei einem informellen Gespräch mit einem guten Glas Wein und Fingerfood in Wohlfühlatmosphäre kennen. Pro Abend verköstigen wir nur 6 Personen aus der Führungsriege.
Thema: Wir besprechen anhand einer fiktiven Firma, wie **eine externe IT-Sicherheitsabteilung** für ein erheblich höheres Sicherheitsniveau sorgen kann. Danach gehen wir gerne auf Fragen ein, wie Ihr Unternehmen dieses erreichen kann.

SICHERN SIE SICH EINEN DER LIMITIERTEN PLÄTZE!

CATERING:	RESTAURANT ZULEGERS
DRINKS:	WEINHANDEL FERTSCH
PRICE:	25,- €
BOARDING:	19:00 UHR / SEATS: 6
DESTINATION:	AUGUSTE-VIKTORIA-STR. 3 D-61231 BAD NAUHEIM

Wir bitten um verbindliche Reservierung unter:
boarding@movetech.net /// T 06032 - 92650

IHRE CREW STELLT SICH VOR
Wir sind Experten in den Bereichen hochsichere VDI-Umgebungen, Datenschutz und IT-Sicherheit. Unser Team besteht aus Hackern, IT-Sicherheitsexperten und Informationssicherheitsmanagern. Unser Ziel ist es, die IT unserer Kunden schnell und unkompliziert auf ein angemessenes Schutzniveau zu bringen. Dabei arbeiten wir rein lösungsorientiert und vor allem leicht verständlich.

SIE WÜNSCHEN EXTERNE UNTERSTÜTZUNG IM BEREICH IT-SICHERHEIT? KONTAKTIEREN SIE UNS:
movetech® IT-Solutions
Auguste-Viktoria-Str. 3
61231 Bad Nauheim
E-Mail: kontakt@movetech.net
Telefon: 06032 92650

Inhaltlich verantwortlich: Gordon Kirstein
Gestaltung: Stefanie Schaffer / www.visuellelogik.de
UNREGELMÄSSIG ERSCHEINENDES INFOMAGAZIN