eBUSINESSLOTSE
INFOBÜRO FÜR UNTERNEHMEN
SCHWABEN

LEITFADEN

Sicherer Betrieb von Unternehmensnetzen

Aufbau, Struktur und Funktionen aller wichtiger Komponenten einfach erklärt

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Sicherer Betrieb von Unternehmensnetzen

Viele Computernetzwerke in Unternehmen wachsen historisch und werden schon deshalb oft unübersichtlich. Zudem wechseln die das Netzwerk betreuenden Mitarbeiter oder sind unerfahren. Das führt häufig dazu, dass Netzwerke nicht optimal und störungsfrei arbeiten. In der Folge kann die Technik die Mitarbeiter nicht optimal bei ihrer Aufgabenerledigung unterstützen. Mit diesem Leitfaden werden die Struktur und die am häufigsten verwendeten Komponenten von Netzwerken vorgestellt und ihre Funktion erklärt

Häufig wachsen Netzwerke mit der Zeit und der Unternehmensentwicklung und werden dann unübersichtlich, schwierig zu warten und dadurch kostenintensiv. Zudem zeichnen sich historisch gewachsene Netzwerke in der Praxis häufig durch mangelnde strukturelle Komponenten aus. Die nächsten Punkte versuchen Ihnen einen Überblick über gängige Komponenten zu vermitteln, zu erklären wie und wo man sie einsetzt und wie sie anhand eines exemplarischen Netzwerkes kombiniert werden können.

Domäne & Domänencontroller (DC)

Oft sieht man in gewachsenen Netzwerken, dass alle Geräte lose miteinander gekoppelt sind und innerhalb des Netzwerks ähnliche Berechtigungen besitzen. Das ist für Administrationszwecke ein nicht wünschenswerter Zustand, da die verantwortliche Person nur schwer einschätzen kann, welcher Mitarbeiter auf welchem System welche Berechti-

gungen besitzt, welche Software installiert hat oder auf welche Daten zugreifen kann.

Um dieses Problem aufzulösen wird in der Praxis ein sog. Domänencontroller verwendet. Unter einer Domäne versteht man in der Praxis ein Computernetzwerk oder Teile davon, welche demselben Sicherheitsbereich angehören. Dieser Sicherheitsbereich zeichnet sich durch eine zentrale Verwaltung aller darin enthaltenen Ressourcen aus.

Im praktischen Einsatz wird dies durch einen so genannten Domänencontroller gelöst. Das ist ein Server mit einem entsprechenden Betriebssystem (häufig Windows Server 20XX), der dafür zuständig ist, das Netzwerk, in dem er sich befindet, zu organisieren. Zu dieser Organisation gehören mehrere Aufgaben wie das Bereitstellen eines zentralen Benutzerverzeichnisses oder die zentrale Verwaltung von Einstellungen auf den verbundenen Rechnern. Damit ein Rechner Teil einer Domäne wird muss er einmalig in diese aufgenommen werden.

Das zentrale Benutzerverzeichnis, das durch den Domänencontroller bereitgestellt wird, ermöglicht es, dass sich jeder darin enthaltene Benutzer an jedem Rechner innerhalb der Domäne anmelden und auf seine Daten zugreifen kann. Ferner lassen sich hier zentral Berechtigungen verwalten, Passwörter zurücksetzen oder Benutzungszeiten von Computern einschränken. Beim Ausscheiden eines Mitarbeiters aus der Firma ist es ausreichend diese Person in dem Benutzerverzeichnis zu sperren, damit er seine kompletten Zugriffsmöglichkeiten innerhalb der gesamten Domäne verliert.

Durch die Möglichkeit Einstellungen zentral zu steuern, kann beispielsweise eingestellt werden, ob die Benutzer USB-Sticks verwenden dürfen, nach wieviel Minuten der Bildschirmschoner aktiviert wird oder nach welchen Zeitraum Kennwörter geändert werden müssen.

Zusätzlich kann durch den Domänencontroller Software von zentraler Stelle aus an die angeschlossenen Rechner verteilt und dort installiert werden.

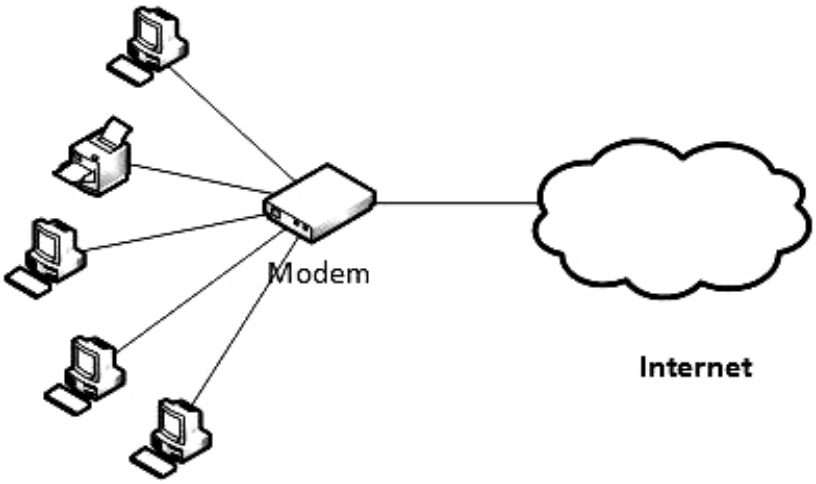


Abbildung 1 historisch gewachsenes Netzwerk

Neben dem kostenpflichtigen Domänencontroller Windows Server von Microsoft existieren auch kostenfreie Alternativen aus dem Open-Source-Bereich. Diese sind jedoch häufig für unerfahrene Administratoren nicht geeignet.

Virenscanner

Die einzelnen Rechner innerhalb einer Domäne sollten gegen Schadsoftware geschützt werden. Dies wird in der Regel durch die Verteilung von Virenscannern an die einzelnen Arbeitsplätze (und ggf. auch Server) realisiert. Diese Verteilung kann ähnlich wie die Verteilung von Software durch den Domänencontroller automatisiert geschehen.

Anders als bei den Virenscannern für Privatpersonen wird im Falle einer erkannten Infektion der Benutzer nicht nach dem weiteren Vorgehen befragt, sondern der lokal im Netzwerk installierte Server für den Virenscanner kontaktiert. Dieser entscheidet dann, anstelle des Benutzers, über das weitere Vorgehen. Dieser Server ist zusätzlich dafür verantwortlich, die lokal installierten Virenscanner mit Updates zu versorgen. Die Effektivität von Virenscannern nimmt mit zunehmender Zeit ohne Updates erheblich ab.

Dadurch dass die einzelnen lokal installierten Virenscanner mit dem Server in regelmäßigen Kontakt stehen kann der Administrator an einer zentralen Stelle

Informationen über den „Gesundheitszustand“ seines Netzes einsehen, Ausnahmen definieren und Updates anstoßen.

In der Praxis sieht man häufig, dass der Server für den Virenscanner auf dem Domänencontroller des Netzwerks installiert wird. (Einige Hersteller empfehlen alternativ den Betrieb eines eigenen Servers hierfür)

Viele Firmen setzen einen Virenscanner von einer der folgenden Firmen ein: Trend Micro, Bit Defender, Kaspersky, Avira, F-Secure, McAfee, Norton (Der alleinige Einsatz des Microsoft-Virenscanners „Security Essentials“ ist für den Schutz eines Firmennetzwerks nicht ausreichend!) Praxistests zeigen, dass kostenpflichtige Virenscannern den kostenfreien Alternativen zum Teil deutlich überlegen sind.

Update

Ein zentraler Sicherheitsaspekt in Firmennetzwerken ist das Aktualisieren von im Einsatz befindlicher Software. Erhebungen zeigen, dass mehr als 80% aller erfolgreichen Angriffe auf Schwachstellen in nicht mehr aktuellen Programmen zurück zu führen sind. Das bedeutet im Umkehrschluss, dass man das Risiko einem zufälligen, erfolgreichen Angriff zum Opfer zu fallen auf 20% senken kann, nur indem man die verwendete Software innerhalb des Firmennetzwerks aktualisiert.

Bei der Aktualisierung wird häufig zwischen zwei Gruppen von Updates unterschieden – zwischen Microsoft-Produkten (Windows, Office, etc…) und Drittanbietersoftware. Microsoft-Software lässt sich innerhalb von Domänen komfortabel durch einen zentralen Update-Server aktualisieren. Dieser Update-Server wird als WSUS-Server bezeichnet. (Windows Server Update Services) Der lokale Administrator kann aus der Gesamtheit aller von Microsoft zur Verfügung gestellten Updates entscheiden welche er an die im Netzwerk befindlichen Clients verteilen möchte.

Um die im System befindliche Drittanbietersoftware (unabhängig von deren eigenen Updatemechanismen) zu aktualisieren werden in der Regel Lösungen spezialisierter Anbieter benötigt.

Regelmäßige Updates in Firmennetzwerken sind ein wichtiges Kriterium für die IT-Sicherheit des gesamten Netzwerks!

Back-Up

In Firmennetzwerken ist die Sicherung von Daten ein zentrales Element, da diese auf diversen Wegen ungewollt verändert oder beschädigt werden können. Dabei reicht das Spektrum von versehentlichem Löschen durch Mitarbeiter über Festplattendefekte oder höhere Gewalt (Feuer, Blitzschlag) bis hin zu Schadsoftware, die Daten verschlüsselt und erst gegen eine Zahlung wieder freigibt.

Bei Datensicherungen unterscheidet man zwischen zwei großen Bereichen die nicht verwechselt werden dürfen, der Historisierung und einer Ausfallsicherheit durch Redundanz.

Im Rahmen der Historisierung soll es möglich sein, den Stand einer speziellen Datei oder eines Ordner so wieder herzustellen, wie er zu einem definierten Zeitpunkt vorlag. Microsoft Windows stellt dazu einen Dienst namens „Volumenschattenkopie“ bereit. Zusätzlich gibt es verschiedene kostenlose und kostenpflichtige Software die den Benutzer dabei unterstützen kann.

Das zweite Sicherungsmodell versucht Ausfallsicherheit durch parallel betriebene Hardware zu realisieren. In der

Praxis werden hierfür in der Regel sog. „RAIDs“ eingesetzt. Das bedeutet, dass Daten die von einem PC an die Festplatte gesendet werden, in Hintergrund auf zwei Festplatten niedergeschrieben werden. Fällt eine der beiden aus übernimmt die zweie Platte mit denselben Daten nahtlos deren Aufgabe. Der Computer bemerkt davon in der Regel nichts.

In der Praxis werden häufig Kombinationen aus beiden Systemen eingesetzt. Da die Anschaffung entsprechender Backup-Systeme mit Kosten verbunden ist sichert man in der Regel nicht alle Rechner eines Unternehmens sondern nur die Server. Um dennoch die Daten der Anwender abzusichern wird häufig pro Anwender ein „persönlicher Ordner“ auf dem Server freigegeben und per Verknüpfung auf dem PC des Anwenders eingebunden. Somit unterliegen alle Daten, die der Anwender in diesen Ordner speichert automatisch der Sicherung.

Bei der Positionierung von Geräten zur Datensicherung sollte darauf geachtet werden, dass diese gegen Zugriff durch Dritte geschützt und in einer anderen Brandschutzzone als die zu sichernden Daten aufgestellt sind.

Dateiserver

Abhängig von der Art des Betriebes kann es notwendig sein eigene Dateiserver zu installieren. Bei diesen Dateiservern handelt es sich um Server, die innerhalb des Netzwerks Ordner und Dateien bereitstellen. Durch Administration dieser Server können Berechtigungen der Benutzer eingeschränkt werden. (z.B. nur lesen oder lesen und schreiben)

Mit Hilfe der im Domänencontroller hinterlegten Benutzerliste kann eingeschränkt werden, wer welche Datei sehen, verändern oder lesen darf. Dies wird häufig mit einem Gruppenkonzept kombiniert. Dabei werden die Accounts mehrerer Personen in Gruppen mit selben Berechtigungen zusammengefasst. (z.B. Geschäftsleitung, Produktion, Vertrieb)

Dateiserver sind häufig mit einer relativ großen Speicherkapazität und RAID-Controllern zur Ausfallsicherheit ausgestattet. Somit bieten sie den Vorteil, dass es eine zentrale Stelle gibt, an der Daten für Backups hinterlegt sind. Somit würde es reichen die Festplatten des Dateiservers zu archivieren um eine komplette Sicherung aller relevanter Daten zu besitzen.

Firewall oder UTM

Die meisten Firmennetzwerke sind heutzutage an einer oder mehreren Stellen mit dem Internet verbunden. Um das Risiko von Angriffen aus dem weltweiten Netz gering zu halten werden durch Firewalls eingehende Verbindungen komplett - oder sofern erforderlich - mit wenigen Ausnahmen unterdrückt. Konventionelle Firewalls besitzen nur relativ wenige Möglichkeiten um Einfluss auf diesen Datenverkehr zu nehmen. Bei den konventionellen Modellen kann häufig nur konfiguriert werden, ob eine Verbindung von außen erlaubt ist und wenn ja, wer im inneren des Firmennetzwerks diese entgegennimmt.

Um diese Defizite zu beheben und den jeweiligen Administratoren ein mächtiges Mittel zur Kontrolle des Netzwerkverkehrs zwischen Internet und Firmennetzwerk an die Hand zu geben wurden Firewalls weiter entwickelt und werden mit erweiterter Funktionalität nun als UTM (Unified Threat Management) bezeichnet. Diese bringen neben der eigentlichen Firewall-Konfiguration häufig folgende Funktionen mit:

- Untersuchung des Internetverkehrs auf Computerviren
- Inhaltsfilterung (z.B. Erotik, Download-Seiten, Internetseiten…)
- Reporting (wer hat wann was im Internet gemacht)
- VPN-Gateway (Computer von außen in das Firmennetzwerk integrieren)

Firewalls selbst werden mittlerweile häufig dafür verwendet, innerhalb des Firmennetzwerks einzelne Bereiche mit

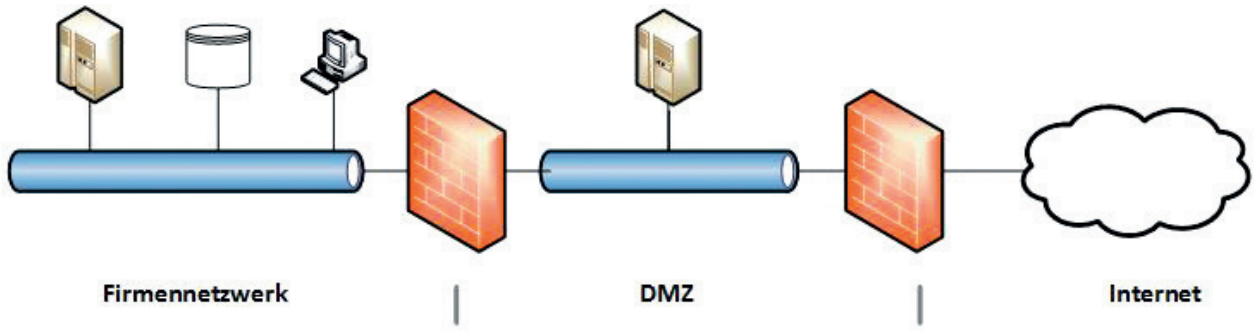


Abbildung 2 DMZ durch Firewall gegen Internet und Firmennetzwerk abgeschottet

selben Vertrauenszonen voneinander abzugrenzen. Dies kann zum Beispiel Sinn machen, um das Netz der Entwicklungsabteilung oder der Personalabteilung weitgehend von den restlichen Büronetzen abzuschotten.

In einigen Fällen kann es vorkommen, dass die Funktionalität von Servern sowohl aus dem Internet als auch aus dem internen Netzwerk benötigt wird. Somit muss der Zugriff von beiden Stellen aus möglich sein. Um dies zu gewährleisten sollte dieser Server durch eine Firewall in Richtung des Internets abgesichert werden und zusätzlich durch eine Firewall in Richtung des internen Netzwerks. Dieser Bereich zwischen Internet und internem Netzwerk, der durch Firewalls getrennt ist wird als DMZ (Demilitarisierte Zone) bezeichnet.

Solche Server in der DMZ könnten beispielsweise Dateiablagen sein, über die die Mitarbeiter mit externen Firmen Dokumente austauschen.

WLAN

Durch WLAN können netzwerkfähige Geräte ohne Kabelverbindung in das Netzwerk der Firma integriert werden. Ein WLAN-Empfänger, der in das Netzwerk integriert wird und als Verbindungsstelle zu den kabellosen Geräten dient wird als „Access Point“ bezeichnet. Während in kleinen Firmen das WLAN häufig wie in Privathaushalten nur mit einem Passwort geschützt ist kombinieren größere Firmen die Anmeldung am Netzwerk häufig mit dem Benutzerverzeichnis auf dem Domänencontroller. Auf diese Weise kann definiert werden, welche Personen berechtigt sind das WLAN zu nutzen. Mit dem Sperren des Accounts einer Person, beispielsweise beim Ausscheiden aus der Firma, erlischt automatisch auch die Zugangsberechtigung zu dem Netzwerk über das WLAN. Wäre das WLAN wie in Privathaushalten oder kleinen Firmen nur mit einem Kennwort gesichert bliebe die Möglichkeit der ausgeschiedenen Person bestehen sich in das Netzwerk zu verbinden. Von einer Änderung des Passworts wären alle Personen (und Geräte!) betroffen, die das entsprechende WLAN nutzen.

Der Server, der die Authentifizierung der Benutzer durchführt, wird als RADIUS-Server bezeichnet und ist bei vielen Domänencontroller n bereits von Haus aus mit an Bord. Die Installation eines entsprechenden WLAN-Netzwerks sollte durch einen erfahrenen Administrator erfolgen!

Drucker und Faxgeräte

Häufig bereiten Drucker und Faxgeräte in historisch gewachsenen Netzwerken Probleme, da diese im Falle eines Defekts oder eines Austauschs durch ein neues Gerät an allen PCs, die damit gearbeitet haben, neu konfiguriert werden müssen. Dafür gibt es in zentral administrierten Netzwerken eine professionellere Lösung:

Die Geräte, die allen Nutzern innerhalb eines Netzwerks zur Verfügung stehen sollen, können an dem Domänencontroller des Netzwerks angegeben wer-

den. Auf diese Weise können die PCs, die mit dem Domänencontroller verbunden sind, automatisch auf diese Geräte zugreifen. Zudem können dadurch an zentraler Stelle Einstellungen wie Papierformat, Wasserzeichen oder Farbeinstellungen konfiguriert werden.

Virtualisierung

In einigen Fällen ist es nicht unbedingt erforderlich, dass ein Rechner oder Server innerhalb eines Netzwerks tatsächlich als physikalisches Gerät existiert. Die Alternative hierzu ist ihn zu virtualisieren. Darunter versteht man seine Festplatte, sein Betriebssystem und seine Funktion in eine so genannte virtuelle Maschine zu verpacken und die durch einen Server hosten zu lassen. Ein solcher Server kann mehrere virtuelle Maschinen gleichzeitig hosten.

Für Virtualisierung kann es mehrere Gründe geben:

- Die Funktionalität eines Servers soll innerhalb eines Netzwerkes weiter zur Verfügung stehen, ohne dass seine Hardware weiter betrieben werden muss. (Beispielsweise wenn die Hardware eines Servers „in die Jahre gekommen“ ist und die Versorgung mit Ersatzteilen in der Zukunft nicht mehr gewährleistet ist)

- Als Ausfallsicherheit: Wenn der Server, der die virtuellen Maschinen hostet ausfällt kann ein anderer Server die Maschinen zur Verfügung stellen, ohne dass für den Benutzer ein Unterschied zu erkennen ist.

- Angenehmes Backup-Verhalten: Der Zustand einer virtuellen Maschine kann auf Knopfdruck gesichert werden und zu einem späteren Zeitpunkt exakt wieder hergestellt werden. Das kann beispielsweise bei Problemen durch Updates oder Virenbefall nützlich sein.

Kombination der Technologien

Durch eine Kombination der vorgestellten Technologien können komplexe, zentral zu administrierende, übersichtliche und professionelle Netzwerke erstellt werden. Dabei spielt es im Prinzip keine Rolle, ob kostenpflichtige Produkte verbreiteter Hersteller oder kostenfreie Open-Source-Alternativen eingesetzt werden. Die Struktur des Netzwerks sowie die in Einsatz befindliche Software und Hardware sollte jedoch hinreichend dokumentiert werden.

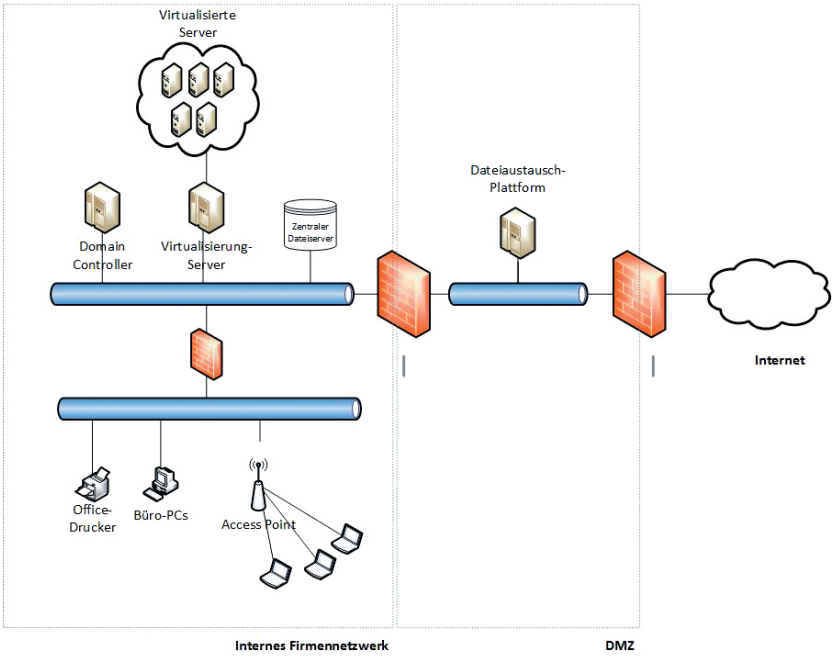


Abbildung 3 Schematisches Firmennetzwerk mit verschiedenen, gängigen Komponenten

Fazit

Die heutigen technischen Möglichkeiten um das eigene Firmennetzwerk und dadurch die Arbeit in diesem zu optimieren sind durch viele technische Hilfsmittel sehr umfangreich. In der Praxis scheitert jedoch eine geeignete Umsetzung häufig an dem Unwissen der verantwortlichen Personen über diese Mittel oder die Scheu unerfahrener Administratoren, sich in neue Technologien einzuarbeiten. Moderne Technologien ermöglichen zudem das eigene Netzwerk gegen verschiedene Bedrohungen zu schützen, die ohne den Einsatz jener erheblichen Schaden anrichten könnten. Es lohnt sich einen Blick auf diese technischen Möglichkeiten zu werfen!

Quellenangaben:
1 | http://www.chip.de/artikel/Virenscanner-Windows-7-20-Programme-im-Test_63365226.html

https://de.wikipedia.org/wiki/RAID

eBUSINESSLOTSE
INFOBÜRO FÜR UNTERNEHMEN
SCHWABEN

Der eBusiness-Lotse Schwaben ist Teil der Förderinitiative „eKompetenz-Netzwerk für Unternehmen“, die im Rahmen des Förderschwerpunkts „Mittelstand-Digital – IKT-Anwendungen in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird. Der Förderschwerpunkt unterstützt gezielt kleine und mittlere Unternehmen (KMU) sowie das Handwerk bei der Entwicklung und Nutzung moderner Informations- und Kommunikationstechnologien (IKT). Mittelstand-Digital setzt sich zusammen aus den Förderinitiativen „eKompetenz-Netzwerk für Unternehmen“ mit 38 eBusiness-Lotsen, „eStandards: Geschäftsprozesse standardisieren, Erfolg sichern“ mit 16 Förderprojekten und „Einfach intuitiv – Usability für den Mittelstand“ mit zurzeit 14 Förderprojekten.

Weitere Informationen finden Sie unter www.mittelstand-digital.de.

eBUSINESSLOTSE
INFOBÜRO FÜR UNTERNEHMEN
SCHWABEN

IT-Fachwissen:
Für die Region. Aus der Region.

Der eBusiness-Lotse Schwaben ist durch seine Nähe zu forschenden Einrichtungen in der Lage, auf tagesaktuelle Entwicklungen aus dem Themengebiet der IT-Sicherheit einzugehen und in diesem Bereich tiefgehend und fundiert zu informieren.

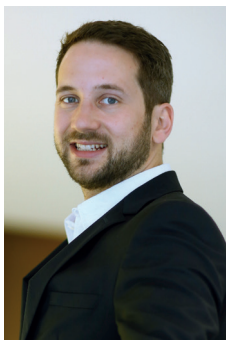
Zu den Mitarbeitern des eBusiness-Lotsen Schwaben gehören unter anderem Mitglieder der HSASec, der Forschungsgruppe IT-Security und Forensik der Hochschule Augsburg. Die Forschungsschwerpunkte der HSASec liegen in den Bereichen des Penetration-Testing, des Secure Software Development Lifecycles sowie der IT-Forensik und der Industrieautomatisierungssicherheit.

Hierbei arbeitet die Forschungsgruppe mit national als auch international tätigen Unternehmen zusammen. Erkenntnisse aus diesen Themengebieten können somit zeit- und praxisnah durch den Lotsen bereitgestellt werden. Dadurch profitieren die Unternehmen im Einzugsgebiet des schwäbischen Lotsen von den Erkenntnissen aus Forschungstätigkeiten, auf die sie unter anderen Umständen keinen Zugriff erhalten hätten.

Der eBusiness-Lotse Schwaben bietet u.a. Informationen zu den sicherheitsrelevanten Themen IT-Sicherheit und Datenschutz an. Ferner werden Informationen zu den Themen Cloud, Social Media, mobile Dienste und mobiles Arbeiten angeboten.


Sebastian Kraemer


Andrea Henkel


Peter Rosina

Partner dieses Leitfadens:

Impressum

Verantwortlicher Redakteur/Herausgeber:
Präsident Prof. Dr.-Ing. Dr. h.c. Hans-Eberhard Schurk
Hochschule für angewandte Wissenschaften Augsburg
An der Hochschule 1
86161 Augsburg
Tel: +49 (0) 821 / 55 86-0
Fax: +49 (0) 821 / 55 86-3222
eMail: info@hs-augsburg.de

Autor:
Sebastian Wolfgang Kraemer, Wissenschaftlicher Mitarbeiter an der Hochschule Augsburg

Zuständige Aufsichtsbehörde:
Bayerisches Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst
80327 München

Rechtsform:
Körperschaft des öffentlichen Rechts

Geschäftsführung:
Präsident Prof. Dr.-Ing. Dr. h.c. Hans-Eberhard Schurk

Ihr Kontakt zu uns:
Fon: +49 (0) 821 / 450 433 - 106
E-Mail: Team@eBusinessLotse-Schwaben.de
www.eBusinessLotse-Schwaben.de

eBusiness-Lotse Schwaben:
c/o IT-Gründerzentrum GmbH
Werner-von-Siemens-Str. 6
D-86159 Augsburg

Redaktion:
Florian Mattler

Gestaltung und Produktion:
Technik & Grafik
Kerstin Meister
Fon: +49 (0) 8238 / 958338
E-Mail: kerstin.meister@technikundgrafik.de

Bildnachweise:
Jamrooferpix, jijomathai, Ivelin Radkov – Fotolia.com