



Der Wettlauf zwischen
Abwehr und Angriff

Inhaltsverzeichnis

Szenario	3
Ziel des Leitfadens	3
Bestandsaufnahme – was ist zu schützen?	4
Priorisierung	5
Ausfallszenarien – was wäre wenn?	6
Anwendungsbeispiel.....	6
Ein Ausflug in die Technologie.....	7
Software-Probleme.....	7
Schutz vor Schaden.....	8
Handlungsempfehlungen – was tun?	8
IT-Sicherheit.....	9
Fahrplan – kontinuierliche Weiterentwicklung eines Sicherheitskonzepts	9
Fazit.....	10

Über den Autor



Jörg von der Heydt ist Channel- und Marketing-Manager Deutschland bei Fortinet und verfügt über langjährige Berufserfahrung im Bereich IT-Sicherheit. Nach seinem Studium der Elektrotechnik an der Uni Dortmund sammelte er bei Unternehmen wie Philips NK (heute Axians), Unisys und ABB umfangreiche Erfahrungen im Netzwerk-Infrastruktur- und Service-Business, bevor er dann bei Herstellern wie Nokia, Smarttrust und zuletzt Check Point zum Security Experten avancierte. Er hat im Laufe seiner Arbeit festgestellt, dass gerade im mittelständischen Bereich erhöhter Bedarf an praxisorientiertem Know-How und an Sicherheitskonzepten besteht, die genau auf diese Unternehmen zugeschnitten sind.

Über Ihre Fragen oder Anregungen freut er sich unter jvdheydt@fortinet.com.

Szenario

Kleine und mittelständische Unternehmen haben – so belegen es zahlreiche Studien – nach wie vor Handlungsbedarf, wenn es um die Einführung und Umsetzung von IT-Sicherheits-Strategien geht. In den meisten Fällen ist zwar das Bewusstsein für bestimmte Maßnahmen (Firewall, Antivirus) vorhanden, die ausreichende Wirkungsweise solcher Abwehrmittel jedoch unklar und nicht dokumentiert. Schlimmer noch – die Auswirkungen bei unzureichenden und/oder falsch eingestellten Verteidigungsstrategien sind häufig nicht bekannt.

Dieses Dokument soll eine Handlungsempfehlung in Form eines 4-Punkte-Plans bieten, der in verständlicher Form die einzelnen Schritte zu einem sinnvollen Sicherheitskonzept aufzeigt, das der Unternehmensgröße angemessen ist.

Die einzelnen Schritte führen von einer Bestandsaufnahme „Was ist zu schützen“ über ein „Was wäre wenn“-Szenario zu einer „Was tun“-Checkliste. Ergänzt wird dies durch einen Fahrplan für die kontinuierliche Entwicklung, der notwendige regelmäßige Maßnahmen NACH der Umsetzung des entsprechenden Konzepts beschreibt.

Ziel des Leitfadens

Ausgehend von direkten Kundenbefragungen, zahllosen Veranstaltungen mit Anwendern, Umfragen, Studien und persönlichen Erfahrungen gelangt der Autor zu dem Schluss: Kleine und mittelständische Unternehmen vernachlässigen die IT-Sicherheit. Und dies aus einem einfachen Grund: Ihnen ist nicht wirklich klar, warum hier Handlungsbedarf besteht. Die aktuellen Bedrohungsszenarien sind den Entscheidern nahezu unbekannt und sie sind sich daher nicht bewusst, wie gefährdet gerade auch mittelständische Betriebe sind. Daher werden auch die Folgen, die sich aus einem Security-Problem ergeben, völlig unterschätzt.

Verpflichtende rechtliche Aspekte sind nur selten Motivation genug, gibt es – bisher – doch keine nennenswerten Referenz-Urteile aufgrund unterlassener Datenschutz-Maßnahmen. Überdies ist hier häufig die Wortwahl bei der Beschreibung solcher juristischen Szenarien unverständlich.

Datenschutzgesetze ergehen sich bis heute nicht in klaren Details und Handlungsanweisungen, die sich in die alltägliche Geschäftspraxis übernehmen lassen – und zeichnen sich ebenfalls häufig durch mangelnde Verständlichkeit aus.

Sogenannte Compliance-Regularien (zu denen Gesetze ebenso gehören wie zum Beispiel Basel II, interne Betriebsvereinbarungen und branchenspezifische Standards) existieren ebenfalls, enthalten aber keine Bedarfsliste oder gar Konfigurationsanweisungen für IT-Sicherheitslösungen.

Die technischen Dokumente der Hersteller und Systemhäuser bedienen sich oft abstrakter Szenarien und einer für Laien unverständlichen Terminologie.

Aber: **Es besteht dringender Handlungsbedarf!**



Die Erfahrung zeigt, dass der unternehmerisch Verantwortliche – also in der Regel der Geschäftsführer oder Inhaber selbst – einerseits Experte in seinem jeweiligen Metier ist (also beispielsweise der Anwalt, der Arzt, der Handwerker, der Dienstleister usw.), andererseits aber die vorhandenen EDV-gestützten Prozesse häufig in ihrer Bedeutung stark unterschätzt.



Ziel dieses Leitfadens ist es daher, einen Schritt VOR dem hypothetischen Schadensfall anzusetzen und die typischen Geschäftsprozesse und ihre Abhängigkeit von elektronischen Medien näher zu betrachten. Nur das Verständnis dieser Zusammenhänge kann nach Ansicht des Autors ein Nachdenken und dann auch ein entsprechendes Handeln bewirken.

Bestandsaufnahme – was ist zu schützen?

Schauen wir uns zunächst die typischen – und vor allem die wichtigen – Geschäftsprozesse in kleinen und mittleren Unternehmen an. In den meisten Fällen sind die folgenden Bereiche wesentlicher Bestandteil der täglichen Arbeit, deren Prozesse überwiegend auf elektronischer Basis abgewickelt werden:

- ☒ Telefonie
- ☒ E-Mail-Versand
- ☒ Kundendatenbank(en)
- ☒ Auftragswesen (Erfassung, Bearbeitung, Rechnungsstellung usw.)
- ☒ Finanzbuchhaltung

Des Weiteren finden sich in Unternehmen jeder Größenordnung in zunehmendem Maße:

- ☒ Unternehmens-Webseiten
- ☒ Online-Shops
- ☒ Elektronische Anbindung an Zulieferer, Kunden oder externe Dienstleister (zum Beispiel Bestellwesen, Abrechnungswesen)
- ☒ Computergestützte Produktionssteuerung
- ☒ Computergestützte Dienstleistung (Grafik-Design, Architektur, Büro-Dienstleistungen usw.)

Nahezu alle Unternehmen beziehen ihre Aufträge und Kundenanfragen telefonisch, per Fax oder via E-Mail – und antworten auf einem dieser Wege. In diesem Fall sind dies die kritischsten und wichtigsten Prozesse neben der Fertigung und Leistungserbringung.

Kundendatenbank und Finanzbuchhaltung können ebenfalls als kritisch angesehen werden, da auch diese Werkzeuge für die tägliche und effektive Erbringung der individuellen Dienst- oder Produktionsleistung erforderlich sind.

Eine Unternehmens-Webseite, die rein informativen Charakter hat, sollte zwar verfügbar sein, hindert aber bei Ausfall niemanden, seiner geschäftlichen Tätigkeit nachzugehen. Je nach Ausrichtung des Unternehmens – also zum Beispiel in der Art der Außenwerbung – kann eine nicht verfügbare Webseite jedoch spürbare Konsequenzen haben.

Ein Online-Shop kann ebenfalls sehr unterschiedliche Bedeutung im Unternehmen haben. Viele Dienstleistungen und Produktionsbereiche können auch online angeboten werden – und in einer zunehmenden Zahl von Unter-

nehmen basiert inzwischen ein großer Teil des Erfolgs auf Online-Business. Printing-on-Demand für Kleinserien, Medikamenten-Versand, Online-Rechtsberatung oder auch Online-Catering-Angebote zur Belieferung von Unternehmen während der Mittagspausen seien stellvertretend für die stark expandierenden Online-Angebote genannt.

Die Anbindung an Zulieferer, zum Beispiel zur „just-in-time“-Bestellung von Produktionsmitteln oder die Anbindung an externe Dienstleister (Abrechnungswesen im medizinischen Bereich, Gehaltsabrechnungen usw.) hat in der Regel ebenfalls sehr hohe Bedeutung für die geschäftlichen Abläufe und deren Erfolg.

Schließlich sei die Erbringung von Dienstleistungen erwähnt, die ausschließlich durch den Einsatz von Computern ermöglicht werden. Hier sind zum Beispiel CAD-Systeme bei Architekten und Konstrukteuren, DTP-Systeme im Bereich Grafik und Werbung oder eine CRM-/CTI-Lösung für CallCenter und Telemarketing-Agenturen zu nennen, die in diesen Fällen sogar den eigentlichen Produktions-Prozess darstellen.

Priorisierung

Aufgabe eines Unternehmers ist es – auch ohne jegliches technisches Verständnis – sein Unternehmen hinsichtlich der etablierten (zum Beispiel der im vorigen Kapitel genannten) Geschäftsprozesse zu analysieren und deren Bedeutung für den Geschäftserfolg zu definieren. Eine mögliche Priorisierung kann folgendermaßen aussehen:

Priorität 1: kritisch

Der Prozess muss während der Arbeitszeiten in jedem Fall verfügbar sein, da ohne diesen die Erbringung (mindestens) einer wesentlichen Leistung nicht möglich ist.

Verfügbarkeit des Prozesses: Sehr hoch

Erforderliche Wiederherstellung: im Bereich weniger Sekunden bis weniger Minuten

Priorität 2: wichtig, aber nicht kritisch

Der Prozess hat große Bedeutung, die ausfallenden Leistungen können aber ohne großen Aufwand nachträglich erbracht werden.

Verfügbarkeit des Prozesses: Hoch

Erforderliche Wiederherstellung: im Bereich weniger Stunden bis max. einen Tag

Priorität 3: weniger wichtig

Der Prozess ist für den Geschäftsalltag von untergeordneter Bedeutung.

Verfügbarkeit des Prozesses: Niedrig

Erforderliche Wiederherstellung: im Bereich weniger Tage

Je nach Größe des Unternehmens sind an dieser Stelle sicherlich individuelle Überlegungen und weitere Abstufungen der Prioritäten erforderlich, für eine erste Einschätzung sollte diese Vorgehensweise jedoch ausreichend sein.

Ausfallszenarien – was wäre wenn?

Nach erfolgter Priorisierung kann jeder Prozess für sich im Rahmen eines „Worst-Case“-Szenarios betrachtet werden – also die Analyse eines Prozessausfalls. Dazu folgende Überlegungen:

- ❑ Welche Abhängigkeit besteht zwischen Geschäftsprozess und elektronischen Systemen?
- ❑ Welche Kosten entstehen bei Ausfall des Prozesses?
 - ▷ Welche Mitarbeiter können dann nicht mehr produktiv sein?
 - ▷ Welche Aufträge können nicht bearbeitet werden oder gehen verloren?
 - ▷ Welche Kosten entstehen für die Wiederherstellung, zum Beispiel Einspielen von Back-ups, Neu-Installation von Software, Beauftragung eines externen Dienstleisters und dessen Kosten (unter Umständen außerhalb der Geschäftszeiten und/oder am Wochenende), Beschaffung von Ersatzgeräten usw.?
- ❑ Welche Auswirkungen eines dedizierten Prozessausfalls hat dieser auf andere Prozesse und welche Folgekosten und -schäden können diese nach sich ziehen (Schadensbegrenzung)?
- ❑ Welche Außenwirkung hat ein Prozessausfall?
 - ▷ Reputation bei Kunden und Geschäftspartnern
 - ▷ Kundenverlust (unter Umständen während einer Angebotsphase / durch Abwanderung zum Mitbewerb)



Anwendungsbeispiel

Ein mittelständisches Unternehmen der Druckbranche hat seine Prozesse optimiert und einen Online-Shop für Print-on-Demand-Aufträge entwickelt. Zur effizienteren Bearbeitung der dadurch entstehenden Angebotsanfragen und Auftragsbearbeitungen (Auftragsbestätigung, Lieferscheine, Rechnungen, Mahnwesen usw.) hat das Unternehmen eine neue Software-Lösung beschafft.

Der Kernprozess in diesem Unternehmen ist zunächst die eigentliche Druckausgabe. Jedoch sind sowohl der Online-Shop, das Auftragsabwicklungs-System als auch das E-Mail-System sowie die allen zugrunde liegende Kundendatenbank unmittelbare Kernprozesse, deren Ausfall schwerwiegende Folgen hätte.

Eine Priorisierung müsste demnach wie folgt aussehen:

- >> Druckprozess(e) = Prio 1
 - >> Auftragswesen = Prio 1
 - >> Online-Shop = Prio 1
 - >> E-Mail-Server = Prio 1
 - >> Kundendatenbank = Prio 1
 - >> Telefonanlage = Prio 2
- usw.

Ein Ausflug in die Technologie

Zum Verständnis der Ursache eines Prozessausfalls ist ein kleiner Ausflug in die Welt der IT-Sicherheit erforderlich. Dieser Leitfaden kann und soll kein vollständiges Kompendium zum Verständnis dieser Thematik sein, jedoch einige wichtige Grundlagen vermitteln, die für die weitere Vorgehensweise hilfreich sind.

Bleiben wir bei dem Beispielunternehmen. Was kann zu einem Ausfall der genannten computergestützten Prozesse führen? Grundsätzlich sind hier zwei Themenfelder relevant: Physikalische Probleme sowie software-basierte Schäden. Physikalische Schäden sind im Tagesablauf meist offensichtlich – und in der Regel auch am besten abgesichert (durch entsprechende Maßnahmen ebenso wie durch Versicherungen). Auf die Vermeidung von Software-Problemen gehen wir im Folgenden näher ein.

Software-Probleme

Offensichtliche Software-Schäden sind solche, die durch Fehler in der Programmierung und/oder der Bedienung entstehen. Ersteres liegt in den Händen des Herstellers, letzteres kann durch entsprechende Schulungen weitgehend vermieden werden. Weniger offensichtliche Schäden entstehen jedoch durch Schad-Software, die über verschiedene Wege ins Unternehmen gelangen kann.

Den höchsten Bekanntheitsgrad haben hier Software-Viren, kleine Programme die bei Ausführung unterschiedliche Effekte zeigen: Löschen von Dokumenten und/oder ganzen Festplatten, Totalausfall eines Computers, unerwünschter Versand von Dokumenten und/oder (Kunden-) Daten via Mail an nicht autorisierte Empfänger.

Neben Viren gibt es weitere schädliche Software, wie zum Beispiel Trojaner, Würmer, Botnets, Scareware und mehr, die ein gemeinsames Ziel verfolgen: Daten und/oder Systeme zu zerstören, zu manipulieren (also zu fälschen) und Daten auszuspähen (also zu sammeln und an Dritte zu verkaufen).

Diese unterschiedlichen Schadprogramme verschaffen sich auf unterschiedlichsten Wegen Zugang zu Endgeräten oder Server-Systemen:

- ❑ durch die Verbreitung via E-Mail (als Anhang oder als Link auf eine schädliche Webseite)
- ❑ über Wirts-Programme (Trojaner-Prinzip), die vordergründig sinnvoll erscheinen, bei deren Ausführung im Hintergrund aber Systeme (Daten, Passwörter usw.) ausgespäht oder gestört werden
- ❑ über manipulierte Webseiten
- ❑ über USB-Sticks, externe mobile Festplatten, digitale Kameras und über Telefone (Smartphones, PDAs usw.), die oft auch via USB-Kabel an PCs angeschlossen werden



Ist ein Schadprogramm aktiv, öffnet es oft weitere „Türen“ (Backdoors) für den unerlaubten Zugriff von außen oder für die Installation weiterer Schadprogramme. In vielen Fällen ist der entstandene Schaden zunächst nicht feststellbar – insbesondere dann, wenn „nur“ Daten ausgespäht oder kopiert werden.

Wichtig ist an dieser Stelle, die möglichen Auswirkungen solcher Schadprogramm im eigenen Unternehmen zu analysieren – in Bezug auf den Ausfall von Prozessen ebenso wie in Bezug auf unter Umständen rechtliche Konsequenzen.

Schutz vor Schaden

Es ist zum Beispiel in Ausbildungsbetrieben und Schulen unbedingt erforderlich, Jugendlichen unter 18 Jahren nur und ausschließlich einen geschützten Internetzugang zu ermöglichen. Ebenso haben unerlaubte Downloads von urheberrechtlich geschützten Daten (zum Beispiel Musik- oder Videodateien, Bücher, Software usw.) rechtliche Konsequenzen für Arbeitgeber.

Auch der unbeabsichtigte Versand von Spam-Mails (der ebenfalls durch Schadprogramme verursacht werden kann) kann zu einer Strafverfolgung oder zu einer „Abschaltung“ des gesamten Mail-Verkehrs des jeweiligen Providers führen. Damit werden ggf. sogar andere Unternehmen in Mitleidenschaft gezogen.

Handlungsempfehlungen – was tun?

Anhand der Beispiele wird offensichtlich, dass und an welchen Stellen im Unternehmen Sicherungsmaßnahmen für Geschäftsprozesse zu ergreifen sind. Dabei ist immer darauf zu achten, dass – insbesondere bei externen Dienstleistern – auch die Haftung im Schadensfall berücksichtigt wird. Dies kann durch das Verfassen sogenannter Service-Level-Agreements (kurz SLAs, diese beschreiben detailliert, wer welche Leistungen zu erbringen hat) zwischen Auftraggeber und -nehmer geregelt werden.



Im Detail bedeutet dies Folgendes:

- ❑ Erstellen eines Konzepts für die Absicherung der entsprechend priorisierten Geschäftsprozesse
 - ▷ Was ist zu schützen?
 - ▷ Wie muss der Schutz im einzelnen aussehen (organisatorisch, physikalisch, EDV-seitig)?
 - ▷ Wer ist für die Durchführung der einzelnen Maßnahmen verantwortlich?
 - ▷ Wer ist für die Einhaltung und regelmäßige Kontrolle der Schutzmaßnahmen verantwortlich?
 - ▷ Welche – unter Umständen vertraglichen – Regelungen sind mit Mitarbeitern in Sachen Datenschutz bereits getroffen oder müssen getroffen werden?
 - ▷ In welchen Abständen wird die Wirksamkeit der Schutzmaßnahmen geprüft?
 - Wer ist verantwortlich für die Prüfung?
 - Wie wird diese durchgeführt?
 - Welche Maßnahmen werden bei Veränderungen/Hinzufügen von Prozessen eingeleitet?
- ❑ Umsetzung des Konzepts gemäß eines entsprechenden Zeitplans
- ❑ Regelmäßige Kontrolle

IT-Sicherheit

In Bezug auf IT-Sicherheit können folgende Handlungsempfehlungen ausgesprochen werden:

- ❑ Benennung und Aus- bzw. regelmäßige Weiterbildung eines oder mehrerer Verantwortlichen/r für IT-Sicherheit
- ❑ Idealerweise Durchführen einer Schwachstellen-Analyse durch einen kompetenten Dienstleister
- ❑ Prüfung und ggf. sukzessive Ergänzung und/oder Ablösung der vorhandenen Sicherheits-Komponenten (Firewall, Antivirus, Intrusion Detection/Prevention Systeme, Anti-Spam-Lösung, Web/URL-Filter, VPN-System(e) usw.) anhand folgender Fragestellungen:
 - Ist die vorhandene Infrastruktur wirksam in der Lage, die aktuellen Schadprogramme abzuwehren ? (kann nur durch Tests und Analysen durch Experten beantwortet werden; eine Aussage anhand von Datenblättern ist an dieser Stelle grob fahrlässig)
 - Handelt es sich bei der vorhandenen Infrastruktur um professionelle Lösungen oder um selbst-programmierte Systeme ? Letztere sind häufig auf einem längst überholten Stand und werden nicht kontinuierlich und dynamisch auf den neuesten Stand gebracht.
 - Werden die vorhandenen Schutzmechanismen regelmäßig und in kurzen Abständen aktualisiert (das Programmieren von Schadprogrammen nach Bekanntwerden einer Schwachstelle dauert mittlerweile nur noch wenige Minuten)
 - Ist die aktuelle Infrastruktur wirtschaftlich vertretbar (Kosten für Updates u.U. vieler verschiedener Systeme, Administration unterschiedlicher Systeme usw.) – oder ist Konsolidierung sinnvoll und/oder erforderlich ?
 - Sind alle Endgeräte ausreichend geschützt (ein Antivirus-Programm allein genügt bei weitem nicht)?
 - Ist eine umfassende sog. Security-Suite installiert (Desktop-Firewall, AntiVirus, IPS/IDS, lokaler URL-Filter für Nutzung außerhalb des Unternehmens, VPN-Client,...) ?
 - Ist diese Lösung zentral oder zumindest komfortabel für mehrere Endgeräte administrierbar ?
 - Wird diese Lösung regelmäßig und automatisch upgedated ?
 - Ist – bei kritischen Daten – die Festplatte verschlüsselt ?
- ❑ Ist der Empfang und der Versand von Mails ausreichend geschützt ?
 - Bei Betrieb eines eigenen Mail-Servers: Ist die Anti-Spam Lösung ausfallsicher und untersucht sowohl eingehende wie ausgehende Mails ?
 - Wird Grey-Listing unterstützt ?
- ❑ Festlegung von regelmäßigen Sicherheits-Checks sowie „Change Management“-Handlungsanweisungen
 - Nach Möglichkeit Erstellung regelmäßiger und automatisierter Reports, die die Verfügbarkeit und Wirksamkeit der Sicherheitsinfrastruktur ausweisen, sowie Durchführung regelmäßiger Analysen über Nutzungsverhalten und Auslastung, die bei Planung und Erweiterung der gesamten Netzinfrastruktur dienlich sind.

Fahrplan – kontinuierliche Weiterentwicklung eines Sicherheitskonzepts

Die regelmäßige Kontrolle eines Sicherheitskonzepts ist essentiell. Ebenso wie die zentralen Geschäftsprozesse (Produktion/Dienstleistung) unterliegen auch EDV-gestützte Begleitprozesse einer kontinuierlichen Entwicklung. Änderungen der EDV-basierten Prozesse selbst sollten dabei hinsichtlich IT-Sicherheitsaspekten kritisch hinterfragt und behandelt werden.

Beispielhaft sei an dieser Stelle auf zwei typische Entwicklungen der IT-Kommunikation hingewiesen: Voice over IP (kurz VoIP, die Telefonie über Datenkabel) und Wireless LAN (kurz WLAN, Funk-Netzwerke). Beide Technologien waren in ihrem Ursprung darauf ausgerichtet, eine bestimmte Kommunikation zu ermöglichen und zu vereinfachen bzw. zu ergänzen. Der Schwerpunkt bei der Entwicklung beider Technologien lag auf der bloßen Bereitstellung dieser neuen Kommunikationswege.

Die ersten Standards und Implementierungen sowohl von WLAN als auch von VoIP ließen Aspekte der IT-Sicherheit gänzlich unberücksichtigt – und das, obwohl beide Technologien viele Angriffspunkte aufweisen. Erst Jahre nach Einführung der jeweiligen Technologie wurden die entsprechenden Standards um dringend notwendige Sicherheitskriterien und -mechanismen erweitert.

Die Einführung einer neuen Software-Lösung im Unternehmen, die Einrichtung eines neuen Aufgaben-Bereichs, Umbaumaßnahmen, neue Kommunikationsmittel (zum Beispiel VoIP oder WLAN, aber auch andere und künftige Technologien) und viele andere Vorgänge können die unter Umständen aufwändig eingeführten Sicherheits-Regularien empfindlich stören oder gar außer Kraft setzen. An dieser Stelle ist es notwendig, einen Prozess zu definieren und zu etablieren, der regelmäßig sämtliche Unternehmens-Prozesse auf Veränderungen analysiert und Auswirkungen auf Verfügbarkeit, Priorisierungen und letztlich auf die IT-Sicherheit dokumentiert. Sich daraus ergebende Maßnahmen sind dann umgehend einzuleiten – und in die weiteren Kontrollen bzgl. der Wirksamkeit des Sicherheitskonzepts einzubeziehen.

Fazit

Die oft als notwendiges Übel verstandene IT-Sicherheit steht in engem und von gegenseitigen Abhängigkeiten geprägtem Zusammenhang mit den vermeintlich wichtigeren zentralen Prozessen eines Unternehmens wie Produktion oder Dienstleistungen. Die für das Unternehmen essentiellen Kernprozesse sind durch entsprechende Maßnahmen abzusichern. Die Entwicklung im IT-Sicherheits-Markt zeigt jedoch, dass der Wettlauf zwischen Abwehr und Angriff unaufhaltsam ist – weshalb der Schwerpunkt auf proaktiven und ganzheitlichen Abwehrmechanismen liegen sollte.

Neben dieser Tendenz sind konsolidierende Maßnahmen auch im häufig heterogenen Umfeld der IT-Sicherheits-Infrastruktur ein verbreiteter Ansatz. Kleine und mittelständische Unternehmen müssen sich dessen bewusst sein oder werden, dass Angriffsszenarien und Schadprogramme unabhängig von der Größe eines Unternehmens entwickelt werden. Dadurch bedingt sind Abwehr-Lösungen notwendig, die entsprechende Technologien bereitstellen und gleichzeitig auch für den Mittelstand kommerziell sinnvoll einsetzbar sind.

Wünschen Sie mehr Informationen?: Fortinet GmbH | T: +49-(0)69-710 423 500 | www.sicher-sein.net | www.fortinet.com