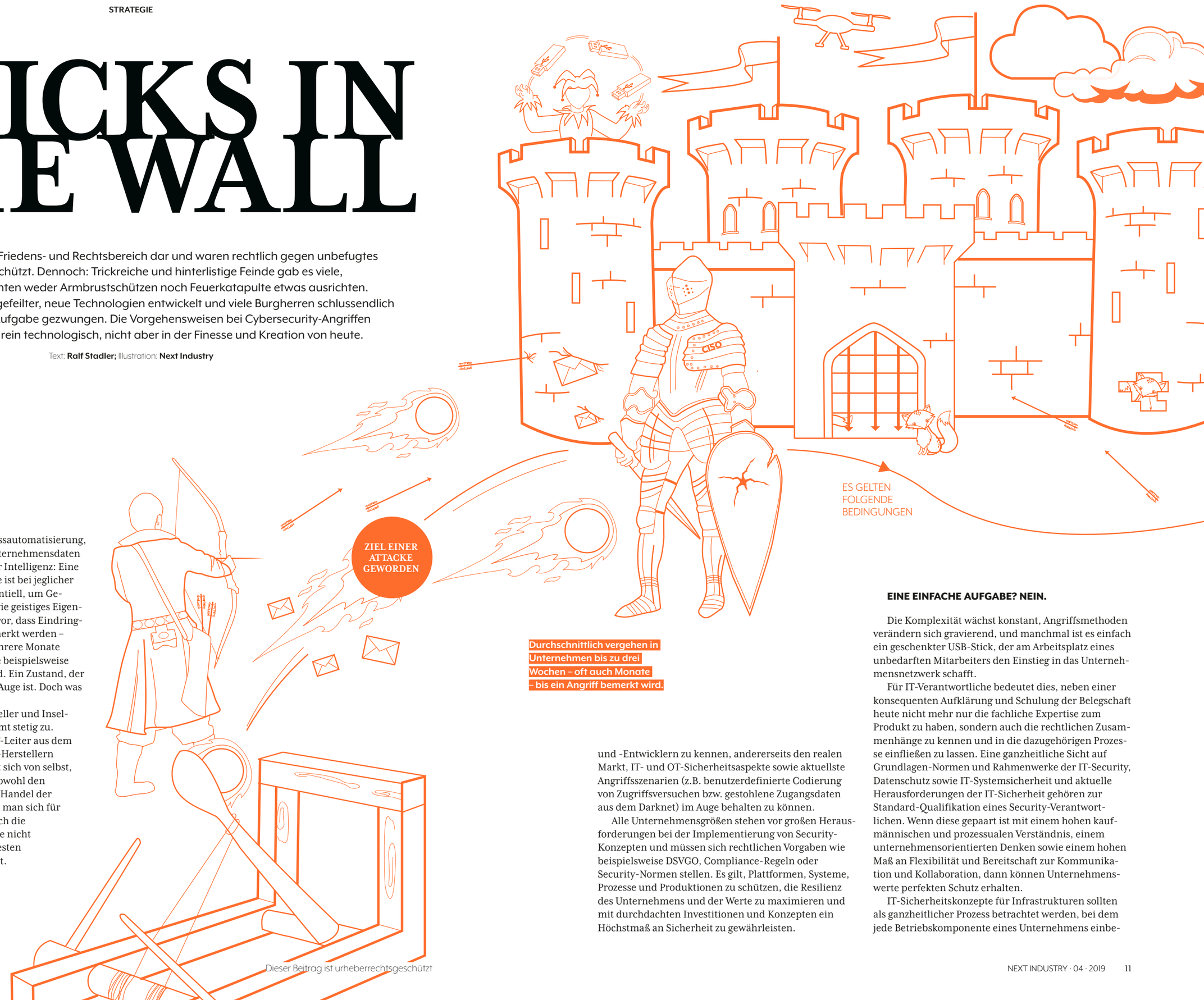
BRICKS IN THE WALL

Burgen stellten einen Friedens- und Rechtsbereich dar und waren rechtlich gegen unbefugtes Eindringen geschützt. Dennoch: Trickreiche und hinterlistige Feinde gab es viele, gegen manche konnten weder Armbrustschützen noch Feuerkatapulte etwas ausrichten. Die Angriffe wurden ausgefeilter, neue Technologien entwickelt und viele Burgherren schlussendlich mit Erpressung zur Aufgabe gezwungen. Die Vorgehensweisen bei Cybersecurity-Angriffen unterscheiden sich rein technologisch, nicht aber in der Finesse und Kreation von heute.

Text: **Ralf Stadler;** Illustration: **Next Industry**



Ob bei der IoT-Anbindung, der Prozessautomatisierung, bei der Analyse von Kunden- und Unternehmensdaten oder der Anwendung von Künstlicher Intelligenz: Eine ganzheitliche Cybersecurity-Strategie ist bei jeglicher Digitalisierung in Unternehmen essentiell, um Geschäftsdaten und Geschäftswerte sowie geistiges Eigentum zu sichern. Zu häufig kommt es vor, dass Eindringlinge oder Cyberattacken zu spät bemerkt werden – Bis zu drei Wochen und auch mal mehrere Monate können vergehen, bis ein Angriff, wie beispielsweise eine Industriespionage, bemerkt wird. Ein Zustand, der CEOs berechtigterweise ein Dorn im Auge ist. Doch was tun?

Die Unübersichtlichkeit der Hersteller und Insellösungen im Bereich IT-Security nimmt stetig zu. Zwischenzeitlich können CIOs und IT-Leiter aus dem Angebot von mehr als 2.000 Security-Herstellern Lösung zusammenstellen. Es versteht sich von selbst, dass bei der Anzahl von Herstellern sowohl den IT-Verantwortlichen als auch dem IT-Handel der perfekte Überblick schwerfällt. Wenn man sich für eine Lösung entschieden hat, stellt sich die Frage, ob beim „Go Live"-Termin diese nicht bereits überholt ist bzw. die allerneuesten Angriffsformen unberücksichtigt lässt.

Als weltweit agierender IT-Distributor haben wir den immensen Vorteil, einerseits die visionären Gedanken und Entwicklungen einer Vielzahl von IT-Herstellern

Durchschnittlich vergehen in Unternehmen bis zu drei Wochen – oft auch Monate – bis ein Angriff bemerkt wird.

und -Entwicklern zu kennen, andererseits den realen Markt, IT- und OT-Sicherheitsaspekte sowie aktuellste Angriffsszenarien (z.B. benutzerdefinierte Codierung von Zugriffsversuchen bzw. gestohlene Zugangsdaten aus dem Darknet) im Auge behalten zu können.

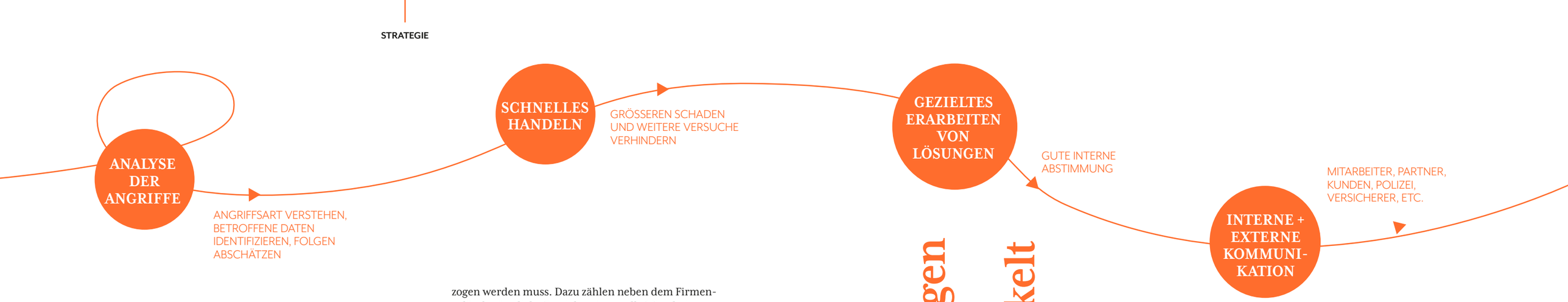
Alle Unternehmensgrößen stehen vor großen Herausforderungen bei der Implementierung von Security-Konzepten und müssen sich rechtlichen Vorgaben wie beispielsweise DSVGO, Compliance-Regeln oder Security-Normen stellen. Es gilt, Plattformen, Systeme, Prozesse und Produktionen zu schützen, die Resilienz des Unternehmens und der Werte zu maximieren und mit durchdachten Investitionen und Konzepten ein Höchstmaß an Sicherheit zu gewährleisten.

EINE EINFACHE AUFGABE? NEIN.

Die Komplexität wächst konstant, Angriffsmethoden verändern sich gravierend, und manchmal ist es einfach ein geschenkter USB-Stick, der am Arbeitsplatz eines unbedarften Mitarbeiters den Einstieg in das Unternehmensnetzwerk schafft.

Für IT-Verantwortliche bedeutet dies, neben einer konsequenten Aufklärung und Schulung der Belegschaft heute nicht mehr nur die fachliche Expertise zum Produkt zu haben, sondern auch die rechtlichen Zusammenhänge zu kennen und in die dazugehörigen Prozesse einfließen zu lassen. Eine ganzheitliche Sicht auf Grundlagen-Normen und Rahmenwerke der IT-Security, Datenschutz sowie IT-Systemsicherheit und aktuelle Herausforderungen der IT-Sicherheit gehören zur Standard-Qualifikation eines Security-Verantwortlichen. Wenn diese gepaart ist mit einem hohen kaufmännischen und prozessualen Verständnis, einem unternehmensorientierten Denken sowie einem hohen Maß an Flexibilität und Bereitschaft zur Kommunikation und Kollaboration, dann können Unternehmenswerte perfekten Schutz erhalten.

IT-Sicherheitskonzepte für Infrastrukturen sollten als ganzheitlicher Prozess betrachtet werden, bei dem jede Betriebskomponente eines Unternehmens einbe-



zogen werden muss. Dazu zählen neben dem Firmengelände sämtliche Betriebsstätten, alle Mitarbeiter sowie das IT-Netzwerk, Kontrollinstanzen, die IT und das Management. Anders gesagt: IT-Security beginnt am Firmentor und endet bei der Entsorgung Ihres Mülls.

Allumfassende Unternehmenssicherheit muss daher ein Mix aus Unternehmensanforderungen und -betrieb, mittel- bis langfristiger Investitionssicherheit sowie interner und externer Ressourcen sein. Denn der eigene Blick auf Security ist nicht immer der vollständige.

WEG VON PROBLEMEN – HIN ZU LÖSUNGEN

Doch wie geht man als IT- oder Sicherheitsverantwortlicher an das Thema heran? Welche Fragen sollten CIOs intern, aber auch ihrem IT-Systemhaus stellen? Wie findet man den perfekten IT-Partner, den Trusted Advisor? Fragen zu stellen ist hierbei immer ein probates Mittel – sich selbst, seinen Mitarbeitern, dem Betriebsrat, aber auch dem IT-Partner. Immer mit dem Ziel, langfristig Ihr größtes Gut – Ihre Daten und Unternehmenswerte – zu schützen.

360°-Ansatz für Security: Wenn Unternehmer es sich einfach machen wollen, empfiehlt sich beispielsweise, auf bewährte ISO-Konzepte zurückzugreifen, mit denen das Qualitätsmanagement in Unternehmen vom Einkauf über die Entwicklung bis hin zu Fachkenntnissen, Endkontrollen und Workflows definiert ist. Ein bewährtes Konzept seit Generationen. Legt man dieses auf Security um, dann lässt sich der Ansatz auf eine Security-Struktur, bestehend aus Firmengelände, Mitarbeiter, IT-Netzwerk, Kontrollinstanzen und Managementinstanz, abbilden.

Wie wichtig ein hohes Prozessverständnis von Fach- und IT-Mitarbeitern ist, zeigt sich bei der Risikoanalyse, bei der es gilt, kritische Geschäftsprozesse zu identifizieren, zu protokollieren und kontinuierlich zu verbessern. In der Produktion betrifft dies beispielsweise ins Netz eingebundene Maschinen und Geräte, zu denen jeweils einzeln die geringsten tolerierbaren Ausfallzeiten definiert sein sollten. Derartige Vorgehensweisen tragen maßgeblich auch zu einer Zertifizierung oder Re-Zertifizierung nach ISO 2700x und anderen Normen (u.a. BSI-Standard 200-X, DSVGO und Grundschutzhandbuch) bei.

Die Sensibilisierung aller Mitarbeiter ist eine wesentliche Voraussetzung für die Umsetzung des gewünschten Sicherheitsniveaus. Die Schaffung der kontinuierlichen Awareness für Security-Themen ist – bedingt dadurch, dass der einzelne Client oder integrierte Sensor oft das Einfallstor für Angriffe von Unternehmen darstellt – essentiell.

ESSENTIELLE FRAGEN ZUR BESTIMMUNG DES STATUS-QUO IHRES SECURITY-KONZEPTS:

Ist Ihr Blick vollständig?

- Zählt Ihr Unternehmen zur KRITIS-Gruppe (spezifische Anforderungen)?
- Welche Systeme mit welchem Softwarezustand haben Sie, und sind sie nach Standards konfiguriert?
- Wie ist Ihr Netzwerk segmentiert und welche Regeln schützen Ihre wertvollen Daten?
- Welche Security-Vorkehrungen wurden bereits getroffen und sind diese Lösungen optimal orchestriert und ausgeschöpft?
- Sind Lösungen gekauft oder bilden Sie diese über Managed Services ab?
- Besteht aktuell eine Bedrohung für Ihre Systeme? Wären Ihre Sicherheitssysteme und Clients darauf vorbereitet?
- Wie sind die Rechte Ihrer User auf ihren Geräten geregelt? Bieten Sie BYOD-Konzepte für Mitarbeiter an?
- Wo befinden sich Ihre wertvollsten Daten? Welche Partner (z.B. Kanzleien) haben darauf Zugriff?
- Benötigen Sie Datenzugriff mit einer 24/7-Verfügbarkeit oder reicht auch 8/5?
- Was machen Ihre Systeme aktuell genau JETZT? Fließen irgendwo unerwünschte Daten?
- Welche Kommunikation findet im Netzwerk statt?
- Wie werden Anomalien gefunden, behandelt und was geschieht mit ihnen, sofern sie eine Bedrohung darstellen?
- Ist Ihr Krisen- und auch Continuity-Management definiert und zumindest im Managementkreis kommuniziert?
- Werden alle Ihre Mitarbeiter regelmäßig zu Themen wie Sicherheit, Compliance und Datenschutz geschult?

»Cyberbedrohungen sind da, bevor Produkte entwickelt werden.«

RALF STADLER, Head of IT-Security bei Tech Data

NOTFALLMANAGEMENT

Wie wichtig die Definition des Prozesses, der nach einem Angriff zu erfolgen hat, ist, finden Unternehmer und IT-Verantwortliche meist erst im konkreten Angriffsfall heraus. Ein seriöses und kontinuierlich aktualisiertes Incident Management, in dem technische und organisatorische Maßnahmen als Reaktion auf erkannte oder potentielle Sicherheitsvorfälle vorgegeben sind, gehört zum Pflichtenheft jedes IT-Leiters. Besonderes Augenmerk sollte auf das Continuity-Management gelegt werden, in dessen Rahmen kritische Geschäftsprozesse im Falle eines Angriffs nicht beeinträchtigt werden oder im Fall einer Unterbrechung (z.B. in der Produktion) eine rasche und sichere Wiederaufnahme von Prozessen sichergestellt wird. Eine hohe Transparenz ist für ein gelungenes Notfallmanagement unerlässlich.

Sollte ein Unternehmen dann doch einmal angegriffen werden, ist eine schnelle Kommunikation, das Inkrafttreten des Krisenplanes sowie die polizeiliche Erfassung unerlässlich. Dass heutzutage nur eine geringe Anzahl der Angriffe gemeldet wird, ist fatal. Denn wenn Informationen über Hacker-Angriffe nicht gemeldet und die Strafverfolgungsbehörden nicht informiert werden, findet auch kein Austausch zu systemischen Optimierungen oder rechtlichen Notwendigkeiten statt. Schlussendlich sehen sich daher Versicherer mangels Transparenz außer Stande, Risiken zu kalkulieren und diese über Policen abzusichern.

Erstaunen löst oft die Antwort auf die Frage aus, welche Unternehmen von KRITIS als zur Gruppe der „Betreiber kritischer Infrastrukturen“ gehörend angesehen sind, bei denen die Resilienz wichtiger Infrastrukturen im Hauptfokus steht. Neben Polizei, Feuerwehr und Militär zählen dazu beispielsweise auch Energieunternehmen, die die Allgemeinheit mit Elektrizität, Gas, Kraftstoffen oder Fernwärme versorgen, oder Branchen wie Informationstechnik, Telekommunikation, Ernährung, Finanz- und Versicherungswesen, Gesundheitswesen, Wasser sowie Transport & Verkehr. Wirft man einen Blick auf die heutige Anbieterstruktur, die neben ein paar großen Anbietern aus einer Vielzahl an Kleinstunternehmen besteht, die z.B. Solar oder Windenergien erzeugen oder die lokale Geothermie betreiben, dann wird schnell klar, dass auch diese Anbieter KRITIS-beauftragt sind.

HILFE BEI DER PARTNERWAHL

Security hat viel mit Vertrauen, aber auch mit Kompetenz zu tun. Umsetzbar sind Lösungen nur mit spezialisiertem Security-Knowhow und einem hohen Verständnis von Unternehmensprozessen und -anforderungen. Die Einbindung von Fachbereichen, der Unternehmensleitung sowie gegebenenfalls einem Betriebsrat ist unerlässlich, um eine gemeinsame Sprache zu sprechen und für Transparenz zu sorgen. Besonders bei der konzeptionellen Erarbeitung und anschließenden Umsetzung und Betreuung eines langfristigen Sicherheitskonzeptes ist der perfekte IT-Partner ein Schlüsselkriterium – sei es ein Systemhaus, ein Managed Service Provider (MSP) oder die eigene Ressource.

Eine wesentliche Kompetenz des Partners sollte die Schaffung von Transparenz sein, und zwar die Transparenz von Prozessen und Abläufen im Unternehmen, von Verantwortlichkeiten und Knowhow-Trägern, von Unternehmenswerten und Compliance-Anforderungen sowie in den verschiedensten IT-Themen wie Infrastruktur, Security-Prozessen, Security-Managed-Services, Security in der Cloud etc..

WAS SIE VON IHREM IT-PARTNER ERWARTEN DÜRFEN

- Evaluierung des weltweiten Security-Portfolios mit Bewertung von Technologie, Marktreife und Skalierbarkeit von Lösungen/ Einschätzung zum Investitionsschutz zur Vermeidung von Fehlinvestition und Supportausfällen
- Transparenz über business- und branchenrelevante Security-Produkte und deren Lösungsqualitäten
- Höchste Qualität bei Lösungsimplementierung, Prozessumsetzung und Einhaltung von Security-Normen und Gesetzen
- Bedarfsanalyse und Angebot an notwendigen Zertifizierungen für interne IT-Mitarbeiter sowie Team-Trainings zur Sensibilisierung
- Anpassung von Betriebsvereinbarungen, Leit- und Richtlinien und ggf. Arbeitsverträgen mit Definition von Prozessen und Verhaltensweisen (Mitarbeiterinformationspflicht unter Einbindung von Betriebsräten)
- Definition und Vergabe des konkret benötigten Supports und gewünschten Abrechnungsmodells für die unterschiedlichen Unternehmensbereiche (z.B. 24/7 für Produktion mit Mehrschichtbetrieb, 8/5 für Administration)
- Beratung zur 100%igen Einhaltung von Compliance-Anforderungen und Security-Normen durch Produkte und zusätzlich erforderliche Prozesse
- Angebot an individuellen, budget- und branchenabhängigen Sicherheitskonzepten auf lokaler oder globaler Ebene mit teils skalierbaren branchenspezifischen Lösungen (S/M/L/XL).
- Angebot eines IT-Security Assessments oder Workshops zum Thema Unternehmenssicherheit und zur schnellen Erkennung von Sicherheitslücken und Prozessmängeln
- Exzellente Vernetzung mit der Distribution, ISVs, Managed Service Providern und Security-Experten

SECURITY BRAUCHT RESSOURCEN

Security-geschulte oder gar zertifizierte Ressourcen innerhalb des Unternehmens aufzubauen und vorzuhalten, ist besonders für den Mittelstand kaum realisierbar. Die interne IT gerät vermehrt an ihre Grenzen, kämpft mit zu wenig Personal bei gleichzeitig steigender Bedrohungslage mit harten Strafen für die Nichteinhaltung von Vorgaben. Eine extrem schwierige Situation, in der Ecosysteme und Service-Partner gefordert sind, um von der Schwachstellensuche und -analyse bis hin zur Forensik alles abzudecken.

Mehr und mehr setzen IT-Leiter darauf, Dienste als Services auszulagern, was auch die Stimmung des Managements aufhellt, wenn CAPEX-Kosten auf OPEX umgebucht werden und das Unternehmen sich auf die Kernaufgaben bzw. die eigene Digitalisierung der Geschäftsprozesse konzentrieren kann. Systemhäuser oder MSPs, die diese Leistungen anbieten, erhalten einerseits einen tiefen Einblick in das Netzwerk des Unternehmens sowie in Prozesse und Strukturen, binden aber andererseits alle Kompetenzträger der Beratungs-, Liefer- und Implementierungskette bis hin zum Betriebsrat mit ein. Ein wichtiger Aspekt bei der Kooperation mit oder Belieferung von größeren Unternehmen und Konzernen.

Doch wo empfiehlt sich eine Auslagerung von Services, welche bieten einen echten Mehrwert? Übernimmt der MSP für den Service auch die Betriebsverantwortung? Welche Hybrid-Modelle funktionieren schon nachweislich? In welchen Fällen ist ein externer Spezialist die günstigere wie auch kompetentere Lösung? Fragen, die wir immer wieder von IT-Verantwortlichen gestellt bekommen und auf die wir auch Antworten haben.

Ein hinsichtlich Security hochqualifizierter MSP wird nach Kenntnis aller Rahmenbedingungen, eventueller Bedrohungslagen und anhand des vom Unternehmen definierten Schutzumfanges entscheiden, welche Technologien er einsetzt. Er entscheidet über die Prozessintegration, über die technologischen Rahmenbedingungen und passt im Hintergrund die Lösungen den Entwicklungen des Unternehmens oder veränderten Angriffsmethoden an.

Zunehmend nachgefragt sind auch Security-as-a-Service Lösungen (SECaaS), bei denen die Lösungen aus dem Rechenzentrum eines Cloud-Providers nahtlos in die Kunden-Infrastruktur integriert und nach Nutzung abgerechnet werden. Unternehmen profitieren u.a. von einer schnellen Bereitstellung und höchster Aktualität der Lösungen sowie von regelmäßigen Audits nach Compliance-Vorgaben, ohne direkt hohe Investitionskosten zu verursachen. Mit SECaaS decken Sie u.a. folgende Security-Segmente ab: Identity Access Management, Mobile Device Management, Vulnerability Management, DDOS Protection, Data Loss Prevention, u.v.m.

ES WAR EINMAL ...

Heute ist gestern. Der extremen Geschwindigkeit an Neuentwicklungen von Hackern zum Angriff auf Unternehmen gilt es mit entsprechender Flexibilität, Expertise und Konsequenz entgegenzuwirken. Durch Technologien wie Cloud Computing in Verbindung mit Industrie 4.0, intelligenter Sensorik, Containering, 5G und neuen Konzepten im Bereich Modern Workplace erhöht sich sowohl die Komplexität der Lösungen als auch das Risiko von Cyberangriffen. Um Imageschäden, Regressforderungen, Produktionsstillständen und Industriespionage vorzubeugen, gilt es, mit den richtigen Partnern, die den Status eines Trusted Advisors verdienen, modernste Sicherheitskonzepte und -implementierungen aufzusetzen, umzusetzen und Mitarbeiter darauf zu trainieren. Denn absolut einmalig in der Welt der Technologie ist die Tatsache, dass Cyberbedrohungen da sind, bevor Produkte entwickelt werden. Damit wäre die Verbindung ins Mittelalter wieder geschlossen, denn auch die Burgherren mussten ein extrem hohes Maß an Flexibilität und Kommunikationsbereitschaft aufwenden, um ihr Volk, ihre Werte und ihre Familien zu schützen. ◄

»IT-Security beginnt am Firmentor und endet bei der sicheren Entsorgung Ihres IT-Mülls.«

Hier gelangen Sie zur Autorenseite mit thematisch passenden Empfehlungen von Ralf Stadler.

Bild: www.frommel.de

Ralf Stadler

... ist international erfahrener und geschätzter Ansprechpartner für Cybersecurity. Bei Tech Data ist er neben seiner Verantwortung für die Geschäftsentwicklung IT-Security in DACH auch weltweit als Hersteller-Scout für Security tätig. Zuvor bekleidete er u.a. bei HPE, Computerlinks (Arrow), ISS (IBM) und Symantec strategische Funktionen.

MEHR DAZU

... finden Sie unter:
www.techdata.de

oder im Tech Data **Channel-Blog** mit Beiträgen zu allen Themengebieten des Distributors:
www.td-live.de