Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT

WERTSCHÖPFUNG DER DIGITALISIERUNG SICHERN

Digitalisierung gilt als die Basis für das Wohlergehen der modernen und globalen Informations- und Wissensgesellschaft. Während sie immer mehr Fahrt aufnimmt, zeigt sie gleichzeitig immer deutlicher auch ihre Kehrseite: Altbewährte Verteidigungssysteme gegen Cyberangriffe versagen zunehmend. Die Ursachen werden inzwischen sehr klar: Der klassische Perimeter löst sich dank Cloud und Mobility auf, die Angriffsflächen werden dank unzähliger neu im Netz hinzugekommener Dinge exponentiell größer, und Abwehrmaßnahmen auf herkömmliche Weise dank einer zerklüfteten, kaum integrierten Security-Landschaft immer komplexer. Zeit, die Erfolgsfaktoren der Digitalisierung zu erkennen und für das eigene Unternehmen umzusetzen. Dabei helfen vier grundsätzliche Cybersicherheitsstrategien.

Digitalisierung eröffnet über alle Branchen und Unternehmensgrößen hinweg enorme Wachstumschancen und führt zu optimalen Prozessen, welche die Effizienz steigern und die Kosten reduzieren. Die neuen Spieler auf dem Feld der Digitalisierung verheißen Großartiges:

- Die Kommunikationsgeschwindigkeiten und -qualitäten, die mit 5G und immer mehr Glasfaser neue Anwendungen möglich machen
- Die Intelligenz der Endgeräte, wie Smartwatches, Smartphones, PADs, IoT-Geräte etc., die viele neue positive Möglichkeiten mit sich bringen
- Aber auch immer leistungsfähigere zentrale IT-Systeme, wie Cloud-Angebote, Hyperscaler, KI-Anwendungen etc., schaffen Innovationen mit großen Potenzialen
- Moderne Benutzerschnittstellen, wie Sprache und Gestik, machen vieles für Nutzer einfacher zu bedienen

Mit all diesen Faktoren lassen sich zähe Business-Prozesse hervorragend optimieren. Das wiederum schafft ein enormes Rationalisierungspotenzial, das es zu heben gilt, um wettbewerbsfähig zu bleiben und Wachstumschancen zu nutzen.

DIE RISIKEN DER CYBERSICHERHEIT STEIGEN STÄNDIG

Leider müssen wir feststellen, dass seit Beginn der IT die Cybersicherheitsprobleme jedes Jahr größer und nicht kleiner werden. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer Endgeräte, Server, Netzkomponenten und zentralen IT-Dienstleistungen nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern für einen erfolgreichen Angriff standzuhalten. Die Vielzahl der lokalen und zentralen Anwendungen, die unterschiedlichen Zugänge zum Internet, die Masse der IT-Systeme etc. erhöhen die Komplexität der IT und damit auch die Anfälligkeit für erfolgreiche Angriffe.

Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität von Software zunutze machen: Malware installieren und damit Passwörter sowie Identitäten stehlen, Endgeräte ausspionieren, die IT-Systeme verschlüsseln und Lösegeld für die notwenigen Schlüssel zu Entschlüsselung erpressen – um nur einige der gängigen Vorge-

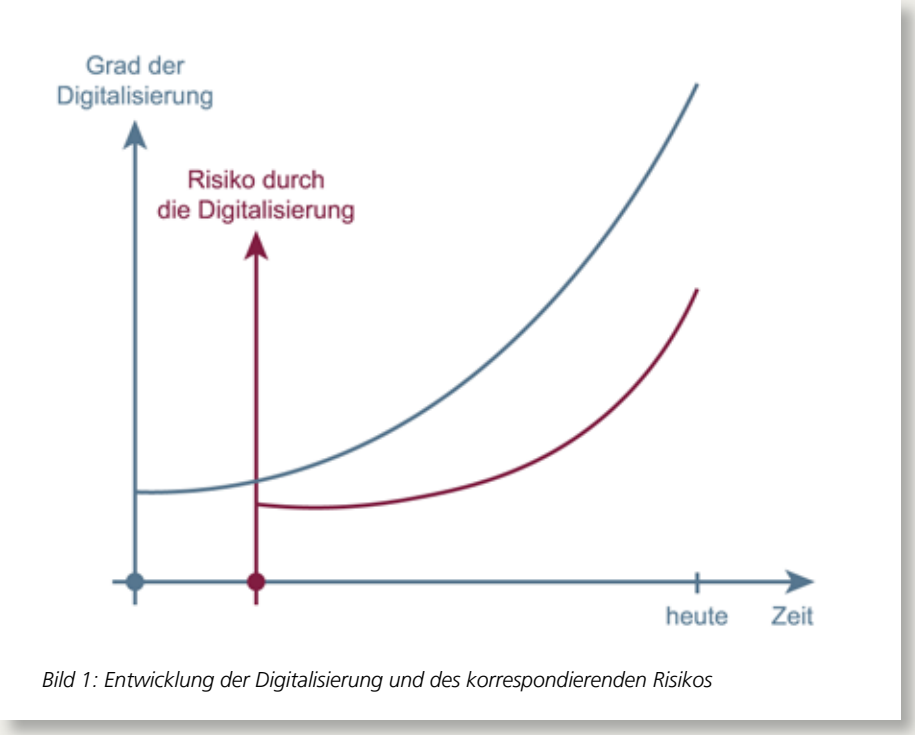

Bild 1: Entwicklung der Digitalisierung und des korrespondierenden Risikos

hensweisen zu nennen. Die Robustheit unserer IT-Systeme ist nicht groß genug und der Level an Cybersicherheit entspricht nicht dem „Stand der Technik". Mit der Digitalisierung wird zurzeit auch das Risiko eines Schadens immer größer (Bild1)!

Ungesicherte IT-Systeme genießen immer noch zu viel Toleranz bei Nutzern und Unternehmen. Diese Einstellung wird sich in Zukunft mit der Bedeutung der Digitalisierung in unserer Gesellschaft radikal ändern müssen, wenn wir die Chancen weiterhin positiv nutzen wollen. Eine angemessene, sichere und vertrauenswürdige IT gemeinsam zu bewältigen, ist für die erfolgreiche Zukunft unserer Informations- und Wissensgesellschaft und insbesondere auch für jedes einzelne Unternehmen entscheidend. Letztlich muss die angestrebte und notwendige Digitalisierung auch die Nachhaltigkeit als strategisches Ziel haben. Das gelingt nur, wenn die IT-Technologien und -Services sicher und vertrauenswürdig aufgebaut und umgesetzt sind.

REDUZIEREN DER CYBERSICHERHEITSRISIKEN

Jeder, der dafür verantwortlich ist, die Werte eines Unternehmen zu schützen, muss sich überlegen, mit welchen Cybersicherheitsstrategien er dieses Ziel erfolgreich erreichen kann. Wenn der Cybersicherheitsverantwortliche nichts tut,

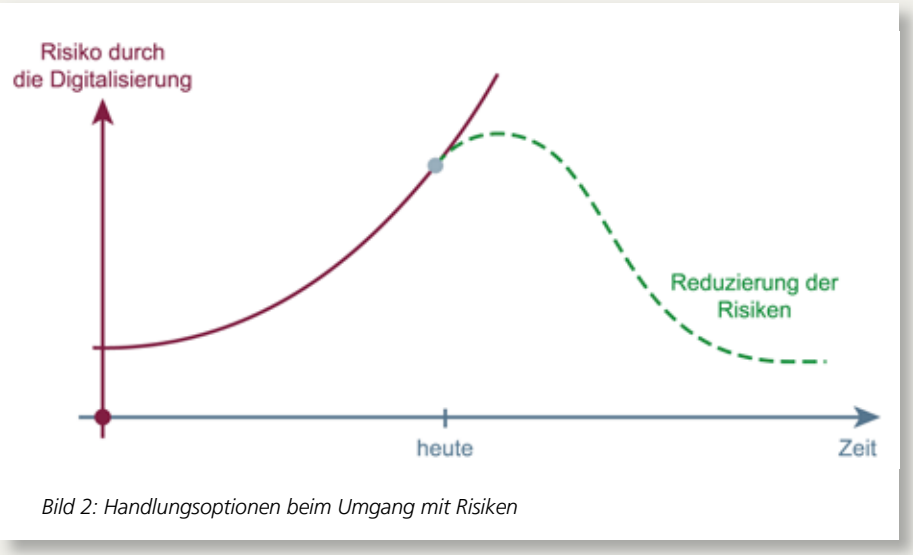

Bild 2: Handlungsoptionen beim Umgang mit Risiken

wird das Risiko eines Schadens mit der steigenden Digitalisierung immer größer (Bild 2, rot Kurve).

Er sollte sich also überlegen, wie er die Cybersicherheitsrisiken strategisch am besten reduzieren kann (Bild 2, grüne Kurve). Dabei werden die Cybersicherheitsstrategien „Vermeiden von Angriffen" und „Entgegenwirken von Angriffen" helfen, den Level an verbleibenden Risiken so klein wie möglich zu halten. Da eine 100 prozentige Cybersicherheit nicht erzielt werden kann – irgendwann überwindet jemand selbst die stärkste Mauer – muss es wirksame Strategien für den Notfall geben. Hier helfen die Cybersicherheitsstrategien „Erkennen von Angriffen" und „Reagieren auf Angriffe".[1]

1. Cybersicherheitsstrategie: Vermeiden von Angriffen

Eine generelle Cybersicherheitsstrategie, die Werte eines Unternehmens zu schützen, ist die Vermeidungsstrategie. Ein Aspekt der Vermeidungsstrategie ist das Prinzip der digitalen Sparsamkeit, das heißt so wenig schützenswerte Daten generieren wie möglich und so viele wie nötig. Daten, die nicht auf IT-Systemen vorhanden sind, können auch nicht angegriffen werden. Durch diese Vorgehensweise werden eine Reduzierung der Angriffsfläche und damit die Reduzierung der Risiken erreicht.

Ein weiteres Prinzip des Vermeidens von Angriffen ist: „Keine Technologien, Produkte und Dienste mit bekannten Schwachstellen verwenden". Dazu müssen natürlich die entsprechenden Schwachstellen bekannt sein. Auch dieses Prinzip hilft, Angriffe zu vermeiden. Beispiele von Technologien, bei denen dieses Prinzip umgesetzt werden kann, sind zum Beispiel Browser, Betriebssysteme und Internet-Dienste. Die Realisierung einer Zwei-Hersteller-Strategie bei Browsern hat beispielsweise den Vorteil, dass wenn ein Browser bekannte Schwachstellen hat, der zweite Browser, ohne bekannte Schwachstelle, weiter verwendet werden kann.

Fokussierung ist ein weiterer Aspekt der Vermeidungsstrategie. Aus Studien ist bekannt, dass im Schnitt fünf Prozent aller vorhandenen Daten in Unternehmen besonders schützenswert sind. Welche fünf Prozent das sind,

Bild 3: Idee der Fokussierung der zu schützenden Werte

wissen die Verantwortlichen in der Regel nicht genau. Aus diesem Grund sollte eine Schutzbedarfsanalyse der vorhandenen IT-Systeme durchgeführt werden, um zu identifizieren, auf welchen IT-Systemen die besonders schützenswerten Daten vorhanden sind. Zugleich lässt sich dabei herausfinden, welche Cybersicherheitsbedürfnisse wie Vertraulichkeit, Authentifikation, Authentizität, Integrität, Verbindlichkeit, Verfügbarkeit und Anonymisierung/Pseudomisierung, erfüllt werden müssen. Damit wären die Verantwortlichen in der Lage, sich auf möglichst wenige IT-Systeme zu konzentrieren und diese wenigen IT-Systeme mit besonders passender Cybersicherheitstechnologie zu schützen. Durch diese Fokussierung können die besonders schützenswerten Daten eines Unternehmens einfacher und besser geschützt werden. In Bild 3 ist angedeutet, dass nur im IT-System in der Mitte besonders sicherheitsrelevante Werte des Unternehmens gespeichert sind, die dann auch besonders geschützt werden müssen.

Sicherheitsbewusstsein zu schaffen ist ein weiterer und wichtiger Punkt der Vermeidungsstrategie. Solche Security Awareness ist das Wissen und die Einstellung, die Mitarbeiter eines Unternehmens zum Schutz der IT mit allen ihren Werten besitzen: Wissen über die Werte eines Unternehmens, die zu schützen sind, den Schutzbedarf der Werte, Bedrohungen, die auf diese Werte wirken, organisatorische Regelungen, die einzuhalten sind, richtige Nutzung von Cybersicherheitsmaßnahmen zum Schutz der Werte etc. und Einstellung bedeutet, dieses Wissen zu verinnerlichen und zum Schutz des Unternehmens aktiv umzusetzen.

BEWERTUNG „VERMEIDUNG VON ANGRIFFEN"

Das Vermeiden von Angriffen ist die beste Cybersicherheitsstrategie, um das Schadpotenzial zu reduzieren.

2. Cybersicherheitsstrategie: Angriffen entgegenwirken

Das Entgegenwirken von Cybersicherheitsmechanismen gegen Angriffe ist die meistverwendete Cybersicherheitsstrategie, um Risiken zu minimieren und damit Schäden zu vermeiden. Es werden Cybersicherheitsmechanismen verwendet, die eine hohe Wirkung gegen bekannte Angriffe zur Verfügung stellen und damit die digital verfügbaren Werte den entsprechenden Cybersicherheitsbedürfnissen gemäß schützen. Ziel ist es, Angriffen erfolgreich entgegenzuwirken und sie damit abzuwehren.

Cybersicherheitsmechanismen, die gegen Angriffe wirken, sind Verschlüsselung (Datei-, Festplatten-, E-Mail-Verschlüsselung, IPSec-Verschlüsselungssysteme, SSL/TLS-Absicherung …), Vertrauensdienste (PKI, Blockchain …), Authentifikationsverfahren, Firewall-Systeme, Anti-Malware-Lösungen, Anti-DDoS-Verfahren, Signaturverfahren, Security Kernel, Isolierung- und Separierungstechnologien, Kompetenz des Nutzers etc.

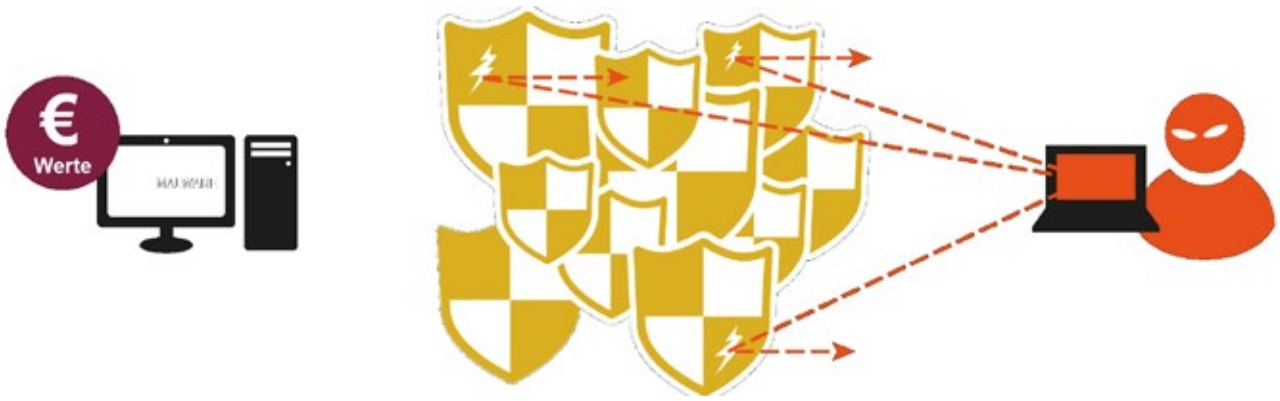

Bild 4: Cybersicherheitsstrategie „Entgegenwirken von Angriffen"

BEWERTUNG „ENTGEGENWIRKEN VON ANGRIFFEN“

Die Cybersicherheitsstrategie „Entgegenwirken von Angriffen“ ist eine naheliegende Vorgehensweise, um digitale Werte angemessen zu schützen. Eine ideale Umsetzung wäre, wenn keine verbleibenden Risiken mehr übrig bleiben würden!

Leider stehen im aktuellen Stand der Technik nicht genug wirkungsvolle Cybersicherheitstechnologien, -lösungen und -produkte zur Verfügung, oder werden nicht angemessen eingesetzt. Da die Cybersicherheitsmechanismen und -lösungen von unterschiedlichen Herstellern kommen, sind sie auch kaum oder gar nicht aufeinander abgestimmt und hinterlassen daher auch noch Schlupflöcher, die von intelligenten Hackern erfolgreich ausgenutzt werden.

Bild 5: Angemessener Sicherheitslevel durch den „Stand der Technik“

„STAND DER TECHNIK“ IM BEREICH DER CYBERSICHERHEIT

Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer Cybersicherheitsmaßnahme, um ein gesetzliches Cybersicherheitsziel zu erreichen.[2]

Das Technologie- und Cybersicherheitsniveau „Stand der Technik“ ist zwischen dem innovativeren Technologiestand „Stand der Wissenschaft und Forschung“ und dem bewährten Technologiestand „allgemein anerkannte Regeln der Technik“ angesiedelt (Bild 5). Cybersicherheitslösungen, die dem Stand der Technik genügen, bieten einen angemessenen Level an Cybersicherheit für den Grad der Digitalisierung.

INTELLIGENTE HACKER, HOPPING CYBERANGRIFFE

Die meisten erfolgreichen Angriffe nutzen die schlechte Wirkung des Entgegenwirkens oder Schlupflöcher und setzten auf sogenannte Hopping Cyberangriffe. Diese Hopping Cyberangriffe werden mehrstufig umgesetzt und oft auch als „Hacker-View“ bezeichnet, weil die Hacker Schrittweise vorgehen und in jeder Stufe kleine Löcher suchen, mit denen sie dann mehrstufig und erfolgreich in eine Firma „hacken“ können.

BEISPIEL EINES MEHRSTUFIGEN ANGRIFFES:

Die Angreifer setzen „Social-Engineering“-Techniken bei Mitarbeitern ein. Social Engineering ist eine zwischenmenschliche Beeinflussung mit dem Ziel, bei Mitarbeitern von Unternehmen bestimmte Verhaltensweisen hervorzurufen, zum Beispiel sie dazu zu motivieren, auf E-Mail-Anhänge oder Links zu klicken.

Wenn die Mitarbeiter das tun, kann unter Ausnutzung von Schwachstellen in der entsprechenden Software als erster Angriffsschritt eine universell verwendbare „Malware“ auf dem IT-System eines entsprechenden Mitarbeiters installiert werden.

Danach kann der Angreifer eine passende Schadfunktionen aus der „Ferne“ in die Malware einbinden und den eigentlichen Angriff mithilfe der Malware durchführen (Bild 6).

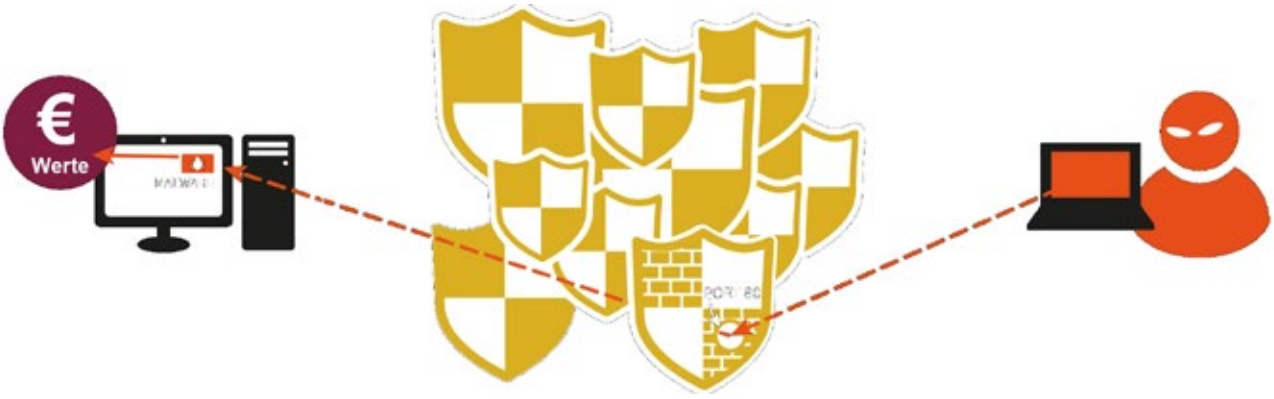

Bild 6: Erfolgreicher „Hopping Cyberangriff“

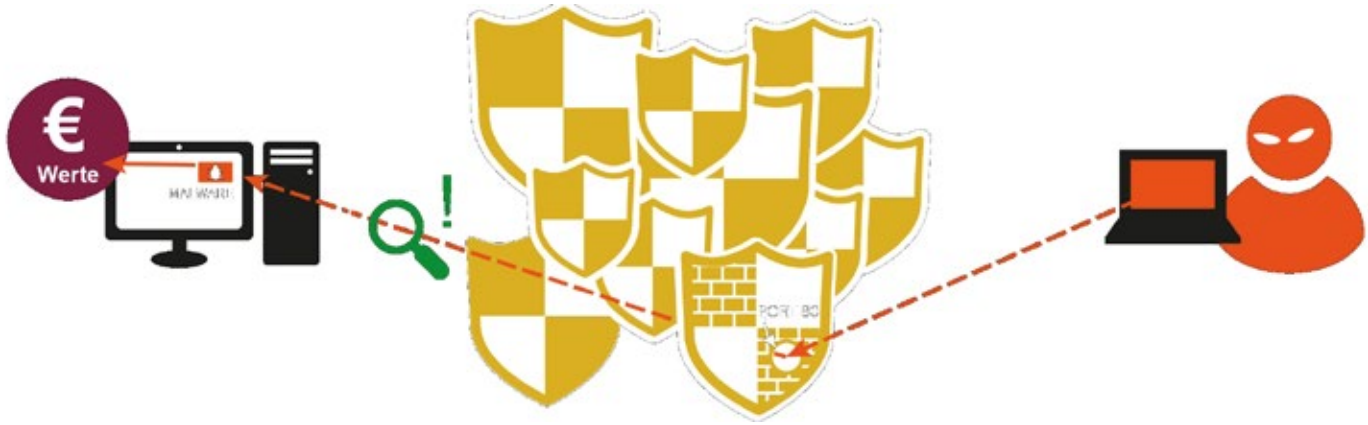

Bild 7: Cybersicherheitsstrategie „Erkennen von Angriffen"

BEWERTUNG „ERKENNEN VON ANGRIFFEN"

Die Cybersicherheitsstrategie, „Erkennen von Angriffen", ist sehr hilfreich, hat aber definierte Grenzen, da es keine 100-prozentige Erkennungsrate gibt. Außerdem muss nach dem Erkennen eine geeignete Reaktion erfolgen, die hilft, den eigentlichen Schaden zu minimieren.

UMGANG MIT VERBLEIBENDEN RISIKEN

Da es immer verbleibende Risiken geben wird, sollen weitere Cybersicherheitsstrategien angewendet werden, die diese beherrschbar machen.

3. Cybersicherheitsstrategie: Erkennen von Angriffen

Wenn sich Angriffe nicht abwehren lassen, bleibt nur noch die Cybersicherheitsstrategie, Angriffe zu erkennen und zu versuchen, so schnell wie möglich zu reagieren, um dadurch den Schaden zu minimieren (Bild 7). In diesem Bereich gibt es zum Beispiel Cybersicherheits-Frühwarn- und Lagebildsysteme, die Warnungen erzeugen, wenn Angriffe erkannt werden. Hier ist die Idee, dass in einem definierten Bereich (Kommunikationsinfrastruktur, Endgeräte …) nach Angriffssignaturen oder Anomalien mit immer mehr Unterstützung von Künstlicher Intelligenz gesucht wird, um dann beim Erkennen dieser entsprechend reagieren zu können, damit Schaden am besten verhindert oder zu mindestens reduziert werden kann.[3]

4. Cybersicherheitsstrategie: Reaktion auf Angriffe

Wenn Angriffe erkannt werden, dann sollte so schnell wie möglich mit passenden Aktionen reagiert werden, die den Schaden im optimalen Fall noch verhindern, zumindest aber die Folgen eindämmen. Wenn ein Angriff erkannt wird, können zum Beispiel sofort Firewall-Regeln so gesteuert werden, dass nur noch die wichtigen Prozesse für das Unternehmen aufrechterhalten bleiben, aber die Angriffsfläche und damit die potenziellen Schäden so gut wie möglich verhindert werden (Bild 8).

Für das komplette Abschalten der Internet-Verbindung oder das Herunterfahren ganzer IT-Systeme, wie bei einem Ransomware-Angriff, muss in der Regel die Frage nach der Verantwortung und der damit verbundenen Rechte definiert sein. Um schneller handeln zu können, müssen die nötigen Informationsflüsse und Reaktionsmöglichkeiten klar ausgearbeitet und vereinbart werden. Wichtig für ein angegriffenes Unternehmen sind ein sehr kurzer Entscheidungsprozess, effiziente Pfade für die Informationsverteilung sowie klar definierte Verantwortlichkeiten, um im Notfall schnell und verantwortungsvoll reagieren zu können. Durch den Einsatz von Cloud-Intelligenz und Machine Learning lassen sich Reaktionen auch in immer stärkerem Maße automatisieren. Auf jeden Fall lässt sich der Angriff analysieren, um dann die vorhandene Lücke zu schließen.

Außerdem sollte die Kommunikationsstrategie zu Mitarbeitern, Kunden, Regulierungsbehörden und Medien sorgfältig geplant werden, um Imageschäden oder gar Strafen – Stichwort DS-GVO – zu vermeiden.

BEWERTUNG „REAGIEREN AUF ANGRIFFE"

Die Cybersicherheitsstrategie „Reagieren auf Angriffe" hilft Schäden zu minimieren oder zu vermeiden. Es kann nur reagiert werden, wenn Angriffe auch erkannt werden. Wichtig ist auch, dass es schon getestete Konzepte gibt, wie Reaktionen umgesetzt werden können und wer die Rechte hat, diese im Angriffsfall auch auszulösen. Alle möglichen Reaktionen sollten sehr gut geübt werden, damit im Ernstfall die passenden Reaktionen auch schnell umgesetzt werden können.

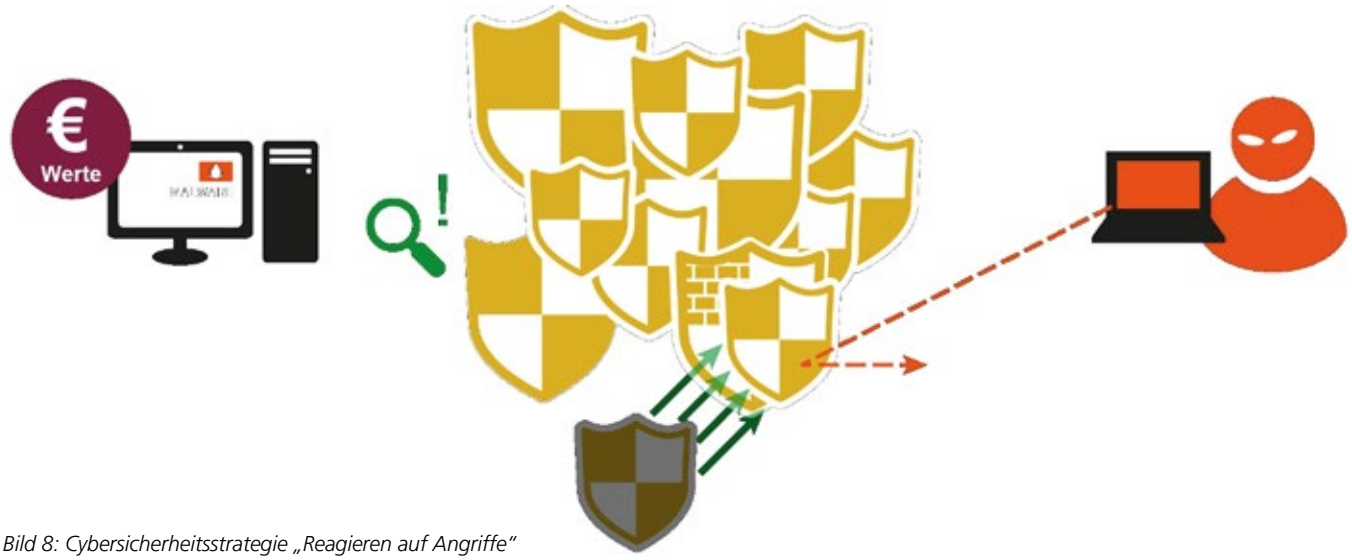

Bild 8: Cybersicherheitsstrategie „Reagieren auf Angriffe"

VON RISIKEN UND RESTRISIKEN

Das Risiko in der Cybersicherheit beschreibt die Wahrscheinlichkeit, mit der eine potenzielle Gefahr, wie ein Angriff auf einen Wert eines Unternehmens, eintritt. Die Eintrittswahrscheinlichkeit hängt zum Beispiel von der Motivation und der Gelegenheit der Angreifer sowie von vorhandenen und nutzbaren Schwachstellen ab.

Risiken können niemals völlig ausgeschlossen werden! Die verbleibenden Restrisiken beschreiben die nach Aufbau einer adäquaten Sicherheitsarchitektur noch vorhandene Wahrscheinlichkeit eines Schadens für das Unternehmen.

CYBERSICHERHEITS-VERSICHERUNGEN

Unternehmen können aber auch Versicherungen als Cyber-Risikoabsicherung abschließen, um einen bedrohlichen Schaden für das Unternehmen zu minimieren. Die Höhe der Deckung der Schäden und die Selbstbeteiligung hängen in der Regel auch von dem Level der Umsetzung der Cybersicherheitsstrategien ab. Je mehr angemessene Cybersicherheitslösungen eigesetzt werden, umso geringer sind die Kosten für eine Cybersicherheitsversicherung.

ZUSAMMENFASSUNG

Die Cybersicherheitsrisiken steigen mit dem Grad der Digitalisierung. Daher sollten die Verantwortlichen für die Cybersicherheit in Unternehmen verschiedene Cybersicherheitsstrategien umsetzen, um das Risiko von Schäden zu reduzieren. Die Cybersicherheitsstrategie „Vermeiden von Angriffen" hilft, Schäden zu reduzieren, hat aber Grenzen in der Umsetzung. Die Cybersicherheitsstrategie „Entgegenwirken von Angriffen" ist sehr naheliegend und erfolgsversprechend. Wichtig ist aber, dass der Stand der Technik verwendet wird, um einen hohen Level an Wirkung gegen intelligente Angriffe zu erreichen.

Die verbleibenden Risiken sollten mit der Cybersicherheitsstrategie „Erkennen von Angriffen" beherrschbar gemacht werden, durch das Identifizieren von gerade stattfindenden Angriffen. Mit der Cybersicherheitsstrategie „Reaktion auf Angriffe" kann dann der Schaden noch verhindert oder zumindest reduziert werden. Cybersicherheitsversicherungen helfen, die verbleibenden Risiken für Unternehmen kalkulierbar zu machen. ■

Quellen:

[1] *N. Pohlmann: „Cybersicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cybersicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019*

[2] *Bundesverband IT-Sicherheit – TeleTrusT: „Handreichung zum – Stand der Technik – technischer und organisatorischer Maßnahmen", Berlin 2020 https://www.teletrust.de/publikationen/broschueren/stand-der-technik/*

[3] *N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit – unausgegoren aber notwendig", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019*

NORBERT POHLMANN,
Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.