LÜNENDONK

Lünendonk®-Whitepaper

Cyber Security

Die digitale Transformation sicher gestalten

Eine Studie der Lünendonk & Hossenfelder GmbH
in Zusammenarbeit mit

arvato
BERTELSMANN
Arvato Systems

Inhaltsverzeichnis

Vorwort

Mario Zillmann, Partner,
Lünendonk & Hossenfelder

Liebe Leserinnen, liebe Leser,

die Wahrnehmung von Cyber-Angriffen und Datensicherheit hat sich in den letzten Jahren spürbar verändert. Infolge der zunehmenden Digitalisierung von Geschäfts- und IT-Prozessen – speziell durch Themen wie digitalen Absatz- und Marketingkanälen oder Internet of Things – nehmen sowohl die Angriffspunkte als auch die Zahl der Angriffe durch Cyber-Kriminalität zu. Eine ganze Reihe von Cyber-Angriffen in den letzten Jahren mit teilweise massiven Prozessstörungen und Datenverlusten spiegeln diese Entwicklung wider. Einfallstore für Hacker waren und sind nicht selten veraltete IT-Landschaften, aber auch eine geringe Priorisierung des Schutzes vor Cyber-Bedrohungen.

Mit fortschreitender Digitalisierung erlangt jedoch der Schutz vor Cyber-Angriffen nun Top-Management-Attention – auch deshalb, weil es neben dem Schutz der eigenen Daten auch immer mehr darum geht, sensible Kundendaten wie Kontakt- und Kontoinformationen zu schützen, die bei der Nutzung digitaler Geschäftsmodelle gesammelt werden. Um ihre IT-Infrastruktur-Ökosysteme künftig besser zu schützen, entscheiden sich immer mehr Unternehmen, ihre Geschäfts- und IT-Prozesse in die Cloud zu verlagern. Während noch vor Jahren vor allem Security-Aspekte gegen eine Cloud-Entscheidung sprachen, hat sich die Wahrnehmung seit einiger Zeit komplett gedreht. Tatsächlich sind Security-Aspekte neben Agilität, Flexibilität und Skalierbarkeit die wichtigsten Gründe für die Auslagerung von IT-Systemen in die Cloud.

Dennoch ist die Nutzung der Cloud kein Rundumsorglos-Paket: So lassen die meisten Unternehmen Teile ihrer Legacy-IT weiter in den klassischen Rechenzentren. Diese hybriden, komplexen IT-Landschaften müssen geschützt werden – vor allem weil kritische Geschäftsprozesse wie Produktion oder Logistik immer stärker IT-gestützt ablaufen und Störungen oder Ausfälle hohen finanziellen Schäden bis hin zum Reputationsverlust verursachen können. Allerdings sind IT-Security-Experten sehr knapp verfügbar, weshalb Unternehmen wirkungsvolle Strategien entwickeln müssen, um dem Spannungsfeld aus Digitalisierungsdruck, Cyber-Kriminalität und Fachkräftemangel zu begegnen.

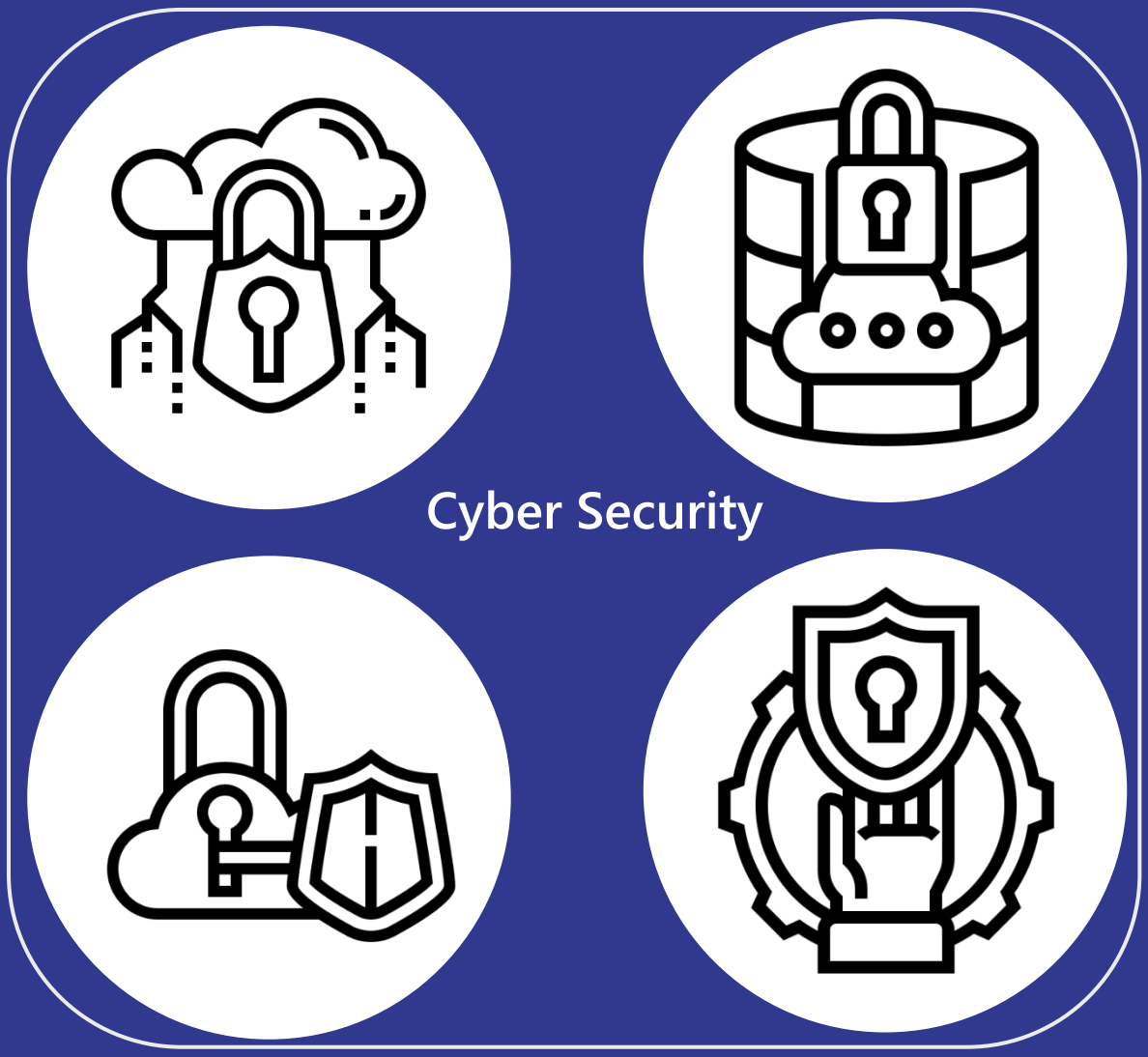
Das vorliegende Lünendonk®-Whitepaper beschäftigt sich mit den Anforderungen an eine nachhaltige Cyber-Security-Strategie. Dieses Whitepaper ist in fachlicher Zusammenarbeit mit Arvato Systems entstanden, für deren Expertise bei der Erstellung des Whitepapers wir uns herzlich bedanken! Wir wünschen Ihnen nun eine interessante und vor allem nützliche Lektüre.

Herzliche Grüße

Mario Zillmann
Partner

„Ohne Cyber-Sicherheit wird Digitalisierung nicht erfolgreich sein."

Bundesamt für Sicherheit in der Informationstechnik (BSI)



Durchbruch bei der Digitalisierung und Plattformökonomie

Die Digitalisierung verändert Unternehmen in unterschiedlichen Bereichen: Branchen sehen sich durch Disruption beziehungsweise neue Wettbewerber mit rein digitalen Angeboten bedroht. Ebenso ändern sich die Anforderungen von Kunden und Mitarbeitern im Zuge der Digitalisierung (Digital Workplace, Digital Experience). Unternehmen investieren daher seit Jahren in die weitere Digitalisierung ihrer Geschäftsmodelle und -prozesse und in den Aufbau komplett neuer, rein digitaler Geschäftsmodelle.

COVID-19 ERHÖHT DEN DIGITALISIERUNGSDRUCK

Der Digitalisierungsdruck wird seit Anfang des Jahres 2020 durch die Covid-19-Pandemie weiter verschärft. Während Investitionen in die digitale Transformation in der Zeit vor Corona zwar getätigt, aber häufig nicht konsequent vollzogen wurden, zeigte der Lockdown mit dem teilweisen Verlust von physischen Absatz- und Kommunikationskanälen notwendige Handlungsfelder auf. Hinzu kommen die Verlagerung von Büroarbeitsplätzen ins Homeoffice und der damit verbundene Durchbruch beim digitalen Arbeitsplatz – inklusive der intensiven Nutzung digitaler Kommunikationstools.

Laut der Lünendonk®-Studie „Digital Efficiency" nimmt mehr als jeder zweite Manager aus großen mittelständischen Unternehmen und Konzernen (54 %) die Covid-19-Krise als eine „große" beziehungsweise „eher große" Bedrohung für sein Unternehmen wahr. Als Konsequenz aus dieser neuen Bedrohungslage werden 48 Prozent der Unternehmen nun infolge der Covid-19-Krise verstärkt in neue, digitale Technologien investieren.

DIGITALE PLATTFORMÖKONOMIE IST ENGÜLTIG AUF DEM VORMARSCH

Die Digitalisierung hat aber nicht nur Auswirkungen auf die Prozesse und die aktuellen Geschäftsmodelle von Unternehmen. Sie ermöglicht auch komplett neue Formen der Zusammenarbeit und der Vermarktung von Produkten und Dienstleistungen. Immer mehr Produkte und Dienstleistungen werden über Onlineplattformen vermarktet, auf die Kunden via Apps auf ihren mobilen Endgeräten beziehungsweise über andere Onlinezugänge zugreifen können. Vor allem in Branchen wie Handel, Finanzdienstleistungen, aber auch immer stärker im industriellen Sektor nimmt der Anteil digitaler Plattformen stetig zu.

Digitalisierung führt zur vollständigen Vernetzung mit dem Internet

Internet of Things & Industrial Internet of Things
- 2020: ca. 30 Millionen mit dem Internet vernetzte Objekte
- Operational Technology (OT) und Information Technology (IT) wachsen zusammen

Digitale Plattformökonomie
- Plattformbasierte Geschäftsmodelle gewinnen weiter Marktanteile
- Mehr als jedes zweite Unternehmen investiert in den kommenden Jahren in Aufbau von plattformbasierten Produkten und Services (API Economy)

Mobile Commerce / E-Commerce
- 2020: ca. 92 Mrd. Euro Umsätze in Deutschland mit E-Commerce (+16%)
- 2020: Mobile Einzelhandelskäufe in Deutschland steigen um 19,9 Prozent auf 34,22 Mrd. Euro.

Cloud Transformation
- 2020: 3 von 4 Unternehmen in Deutschland nutzen die Cloud
- Mehr als jedes zweite Unternehmen migriert seine Legacy-Landschaft in die Cloud
- Public Cloud ist mittlerweile das am häufigsten genutzte Bereitstellungsmodell
- Regulatorik fordert Cloud-Governance

Mobile Enterprise
- 2019: Die Anzahl der Smartphone-Nutzer in Deutschland beläuft sich auf rund 58 Millionen.
- Rund 94 Prozent der großen Unternehmen stellen Beschäftigten mobile Geräte mit Internetverbindung für geschäftliche Zwecke zur Verfügung.

Digital Workplace
- Covid-19-Krise verlagert Büroarbeitsplätze in das Home Office
- Verteiltes Arbeiten wird Alltag
- Anbindung von beruflichen & privaten Endgeräten in die Unternehmensprozesse und IT-Systeme ist große Herausforderung
- Kommunikation findet zunehmend mit cloudbasierten Collaboration Tools statt

Abbildung 1: Entwicklung der Digitalisierung in Deutschland; Quelle: Lünendonk

Tatsächlich legen 51 Prozent der Unternehmen in den kommenden Jahren einen großen bis sehr großen Fokus darauf, Teil der digitalen Plattformökonomie zu werden. Dafür notwendig sind in technischer Hinsicht vor allem schnittstellenoffene IT-Systeme, die eine hohe Interoperabilität mit anderen Unternehmen beim Datenaustausch ermöglichen (Open Source, APIs), die Entwicklung von Cloud-native-Softwareprodukten, um verschiedene digitale Lösungen einfach miteinander zu einer End-to-End-Lösung zu verknüpfen, und die Verlagerung von Geschäfts- und IT-Prozessen in die Cloud, um einerseits von der Innovationskraft von Cloud-Anbietern zu profitieren und andererseits Skalierungsvorteile zu nutzen.

WEITERE BEREICHE VON INVESTITIONEN IN DIGITALISIERUNG

Neben dem Aufbau digitaler Ökosysteme beschäftigt sich ein großer Teil der Unternehmen in den kommenden zwei Jahren sehr intensiv mit der Entwicklung von Innovationen und neuen Geschäftsmodellen (34 %) wie auch mit dem Thema Operational Excellence (28 %). Daneben legen 62 Prozent der Unternehmen einen großen bis sehr großen Fokus auf schnittstellenoffene IT-Prozesse.

Die Digitalisierung findet in sämtlichen Bereichen des öffentlichen und wirtschaftlichen Umfeldes statt und führt dazu, dass zum einen immer mehr Geschäftsvorfälle online (über Plattformen) abgewickelt werden und zum anderen die Zahl der mit dem Internet verbundenen IT-Systeme und Geräte zunimmt. Im Zuge der exponentiellen Technologieentwicklung, wie sie Moore's Law beschreibt, verdoppelt sich die Rechenleistung etwa alle 18 Monate. In der Folge fallen die Kosten für Informationstechnologie und Business Cases für den Einsatz digitaler Technologien wie Cloud Computing, Künstliche Intelligenz oder Internet of Things und werden rentabler beziehungsweise Investitionen amortisieren sich schneller. Es ist daher für die Zukunft weiter davon auszugehen, dass mit zunehmendem Technologiefortschritt auch die Vernetzung von Daten, Objekten, IT-Systemen und Maschinen/Anlagen exponentiell ansteigt. Im Gegenzug nimmt aber auch die Abhängigkeit der Unternehmen von reibungslos funktionierenden IT-basierten Geschäftsprozessen und IT-Infrastrukturen deutlich zu.

FOKUS VON DIGITALISIERUNGSSTRATEGIEN 2020-2021

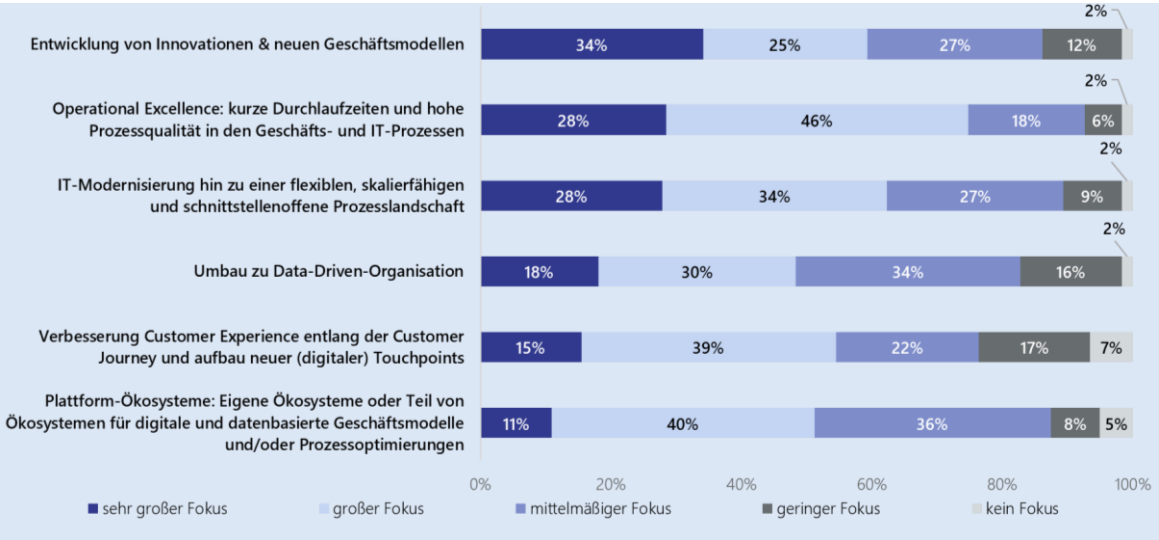


Abbildung 2: Frage: Welchen Fokus nimmt die Digitalisierung in Ihrem Unternehmen in den kommenden 24 Monaten ein? Skala von 1 = „kein Fokus" bis 5 = „sehr großer Fokus"; n = 120 bis 123; Quelle: Lünendonk®-Studie „Digital Efficiency"

Digitale Technologien bieten neue Angriffsflächen

Die digitale Transformation rückt die Informationssicherheit und die Cyber Security nun deutlich stärker in den Vordergrund. Beide Themen gehören jedoch nicht nur in die Verantwortung der IT-Abteilung, sondern müssen CxO Attention haben. Denn durch das Zusammenwachsen aus Business und IT ergeben sich nicht nur neue Potenziale für neues Wachstum durch digitale Geschäftsmodelle und mehr Effizienz durch Automatisierung, sondern eben auch eine ganz neue Bewertung der digitalen Bedrohungslage.

Vor allem der mobile Zugriff auf digitale Anwendungen und sensible Unternehmensinformationen – vor allem im Zuge der Covid-19-Krise – geht mit neuen Sicherheitsgefahren einher. Über die Cloud-Transformation hinaus gibt es noch eine Reihe von digitalen Technologien, die dazu führen, dass Unternehmen ihre IT-Security-Architekturen umbauen müssen.

INTERNET OF THINGS

Die meisten IoT-Geräte sind primär für den Massenmarkt produziert, weshalb die User Experience bei vielen Geräten gegenüber dem Schutz vor Hacking im Vordergrund steht. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) werden viele Systeme in einem unsicheren Zustand ausgeliefert und zahlreiche Hersteller führen keine oder nur sehr selten Sicherheits-Updates oder Fehlerbehebungen durch. IoT-Geräte im privaten Gebrauch bieten also eine gute Angriffsfläche – vor allem wenn sie Zugang zu den mobilen Endgeräten der Benutzer bieten.

API ECONOMY/PLATTFORMÖKOSYSTEME

Immer mehr Unternehmen sehen sich mit der aufkommenden digitalen Plattformökonomie und digitalen Geschäftsmodellen konfrontiert. In einigen Branchen wie Handel und Finanzdienstleistungen setzen Start-ups und Tech-Konzerne die etablierten Anbieter mit digitalen Touchpoints unter Druck. Vor allem die Ausbreitung mobiler Endgeräte und Innovationen im Digitalgeschäft haben die Anforderungen vieler Kunden an die User Experience und damit an die Interfaces zwischen Anbietern und Kunden radikal verändert. Neue Produkte und Services bestehen folglich zu einem immer größeren Teil aus Software und werden zunehmend über digitale Plattformen vermarket. Letztere basieren auf Cloud Computing, Data Analytics und vor allem auf Schnittstellenoffenheit, um eine hohe Integrationsfähigkeit verschiedener digitaler Lösungen zu gewährleisten.

MOBILE ENTERPRISE/DIGITAL WORKPLACE

Spätestens die Covid-19-Krise hat den Digital Workplace auf der Prioritätenliste von Unternehmen ganz nach oben geschoben. Nicht nur im Zuge von Business Continuity Management, sondern auch um agiles Arbeiten und die Work-Life-Balance stärker zu ermöglichen, schaffen nun deutlich mehr Unternehmen Strukturen für verteiltes Arbeiten. Da die meisten Unternehmen in den letzten Jahren jedoch mit der Umstellung auf digitale Arbeitsplätze gezögert haben, stehen sie nun unter enormen Druck, performante und sichere Netzwerke aufzubauen.

Die bisherigen IT-Architekturen haben sich in der Vergangenheit allerdings sehr stark auf abgesicherte Unternehmensnetzwerke bezogen und greifen nun nicht mehr. Die Investitionsplanungen von Unternehmen lassen darauf schließen, dass sich in den kommenden Jahren Software as a Service vollständig durchsetzen und die Zusammenarbeit zu einem überwiegenden Teil via Collaboration-Tools erfolgt wird. Demnach werden immer mehr betriebliche Anwendungen aus der Cloud

genutzt. Konzepte zur Endpoint Security gewinnen im Mobile Enterprise und Digital Workplace folglich enorm an Relevanz, da dadurch die verschiedenen genutzten mobilen Endgeräte mit der Unternehmens-IT zu einem Netzwerk zusammengefasst werden. Handlungsdruck für Unternehmen besteht auch deshalb, weil auf mobilen Endgeräten eine Vielzahl vertraulicher Unternehmensdaten gespeichert wird, beispielsweise Kontakte, E-Mails oder Kundendaten, auf die es die Angreifer abgesehen haben. Die Wahrscheinlichkeit eines gezielten betrügerischen Angriffs auf Mitarbeiter (Phishing) auf mobilen Plattformen ist laut IT-Security-Experten dreimal so hoch wie am Arbeitsplatzrechner. In diesem Zusammenhang gewinnt das sogenannte Zero-Trust-Modell als Sicherheitskonzept enorm an Bedeutung: Bei diesem Modell geht es darum, keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen. Zero Trust weitet die Sicherheitskonzepte somit vom eigenen Unternehmen auf das gesamte Ökosystem aus. Kern des Modells ist die 2-Faktor-Authentifzierung sämtlicher Anwender und Dienste.

DIGITALE TECHNOLOGIEN FÜHREN ZU EINER HÖHEREN RELEVANZ VON CYBER SECURITY

Abbildung 3: Treiber der Cyber Security; Quelle: Lünendonk

DIGITAL FACTORY/INDUSTRIAL INTERNET OF THINGS

Das explosionsartige Wachstum der mit dem Internet verbundenen Dinge und Objekte (Internet of Things) hat die Sicherheitslücken in den Unternehmen dramatisch erhöht – vor allem in Branchen mit kritischen OT-Prozessen (Operational Technology) und IT-Netzwerken. Gleichzeitig vernetzen sich OT und IT im Zuge der vierten industriellen Revolution (Industrie 4.0) immer stärker, wodurch sich – über die IT-Systeme als Einfallstor – neue Angriffspunkte auf kritische Infrastrukturen und Produktionsstätten ergeben und die Versorgungslage gefährden können. Problematisch bei der Industrie 4.0 ist allerdings, dass die eingesetzten OT- und IT-Systeme oft über Jahrzehnte gewachsen sind und der Fokus bei ihrer Entwicklung nicht auf Collaboration und Security gelegt wurde.

CLOUD TRANSFORMATION

Die Cloud ist die zentrale Basis für die eben beschriebenen Technologien und digitalen Geschäftsmodelle. Sowohl die Prozesse als auch die Daten, die aus den digitalen Geschäftsmodellen und -prozessen kontinuierlich generiert werden, liegen zu einem großen Teil in der Cloud. Während die Private Cloud zwar Vorteile im Hinblick auf Datensouveränität bietet, ist sie beispielsweise für Anwendungen wie Machine Learning oder DevOps nicht immer geeignet. Weil seit Corona immer mehr Unternehmen stärker in die Entwicklung und Umsetzung von Digitalisierungsstrategien investieren, nimmt der Innovations- und Time-to-Market-Druck zu. Der Innovationskraft der Public-Cloud-Anbieter, der sogenannten Hyperscaler Amazon Web Services (AWS), Microsoft Azure und Google Cloud, können sich nun immer mehr Unternehmen nicht mehr verschließen und verlagern Teile ihrer Anwendungen in die Public Cloud.

Zahlen & Fakten zur Cyber Security

Die drei Top-Gründe, warum Cyber Security wichtiger wird

*Quelle TÜV-Verband

1. Digitalisierung
2. Öffentliche Wahrnehmung gegenüber Cyberangriffen
3. IT-Sicherheitsvorfälle in den Unternehmen

Schaden durch Cyber-Kriminalität in der deutschen Industrie 2019

*Quelle Bitkom

Zwischen 2018-2019 verzeichnete das BSI 114 Millionen neue Schadprogramm-Varianten

Die wichtigsten Einfallstore für Cyber-Kriminelle

*Quelle: BSI

93% Veraltete IT-Systeme & fehlerhafte Codes

Manipulation der Mitarbeiter durch Social Engineering

Mobile Endgeräte und Apps sind nicht gut genug geschützt

der Unternehmen sehen in Cyberangriffen eine ernste Gefahr für Wirtschaft und Gesellschaft

*Quelle TÜV-Verband

59 Prozent der Unternehmen investieren 2021 in Cyber Security

*Quelle: Lünendonk

55 Prozent der Unternehmen migrieren ihre Legacy-IT in die Cloud wegen höherer Sicherheitsstandards

*Quelle: Lünendonk

LÜNENDONK

Cloud Transformation und Cloud Security

Die Cloud ist der zentrale technologische Treiber für die Digitalisierung. Es ist aber durchaus ein Paradoxon, dass sich zwar eine Mehrheit der Unternehmen aus Gründen der Agilität, Skalierbarkeit und IT-Sicherheit für die Cloud entscheidet, aber die Gefahr externer Angriffe zu den größten Risiken einer Cloud-Migration zählt.

Tatsächlich zeigen mehrere Lünendonk®-Studien, dass große mittelständische Unternehmen und Konzerne immer mehr On-Premise-Anwendungen in die Cloud migrieren. Dabei geht es schon lange nicht mehr nur um IT-Infrastruktur, sondern auch um geschäftskritische Business-Anwendungen wie Product Lifecycle Management (PLM), Manufacturing Execution System (MES), Customer Relationship Management (CRM) oder Enterprise Resource Planning (ERP). Selbst Individualsoftware, die historisch sehr eng mit den Kernprozessen verknüpft sind, werden nach und nach in die Cloud migriert, um anschließend modernisiert zu werden – beispielsweise indem sie auf eine neue technologische Basis verschoben werden.

55 Prozent der befragten CIOs und IT-Manager entscheiden sich laut der Lünendonk®-Studie 2019 „IT-Strategien und Cloud-Sourcing im Zuge des digitalen Wandels" vor allem aus Gründen einer höheren IT-Sicherheit für die (Public) Cloud. Interessanterweise werden die Sicherheitsstandards in der Cloud von immer mehr CIOs als besser eingeschätzt als die in klassischen Rechenzentrumsumgebungen. Beispielsweise nutzen die Hyperscaler, aber auch andere Cloud-Anbieter und Managed Cloud Service Provider, in größerem Umfang künstliche Intelligenz wie Machine Learning, um Datenströme in Echtzeit analysieren und Netzwerkanomalien im Datenstrom erkennen zu können, bevor ein Sicherheitsfall überhaupt eintritt. Je besser die KI trainiert ist – und hier profitieren die Hyperscaler von der steigenden Zahl ausgelagerter IT-Anwendungen und Kunden –, desto genauer werden die Machine-Learning-Modelle und können beispielsweise zwischen schädlichen und nicht schädlichen Dateien unterscheiden oder dubiose Quellen frühzeitig identifizieren und blocken. Hinzu kommt das kontinuierliche, transparente Dokumentieren und Reporting von Cyber Security-KPIs, um jederzeit Auskunft darüber geben zu können, ob die geforderten Security Levels eingehalten werden.

Aber auch die Kontroll- und Steuerungsmöglichkeiten für den Kunden sind in der Public Cloud beziehungsweise in einer gemanagten Cloud deutlich granularer und Kunden können sich ihr eigenes Governance-Modell anlegen, durch das sie umfassende Kontrollmöglichkeiten bei gleichzeitiger enorm hoher Skalierung der Prozesse erreichen.

GRÜNDE FÜR DIE VERLAGERUNG VON ANWENDUNGEN IN DIE CLOUD

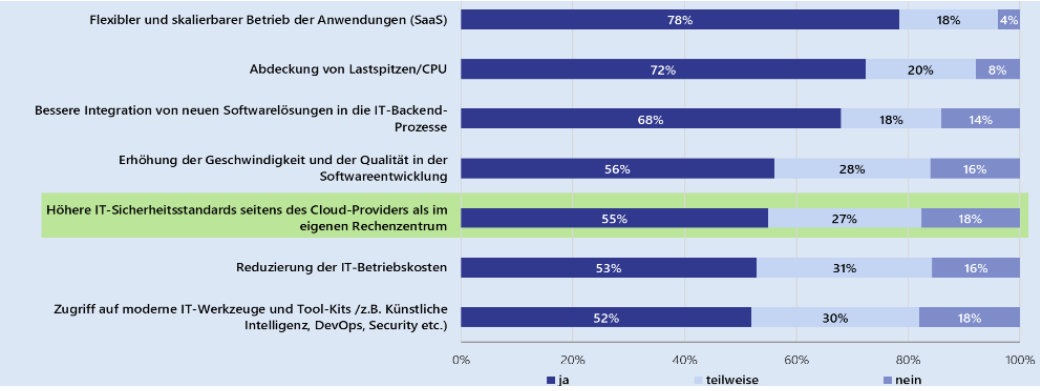


Abbildung 4: Frage: Was sind die Gründe, warum Ihr Unternehmen Anwendungen in die Cloud verlagert bzw. aus der Cloud bezieht (Public und Privat Cloud)? n = 50; Quelle: Lünendonk®-Studie 2019 „IT-Strategien und Cloud-Sourcing im Zuge des digitalen Wandels"

MIGRATION IN PUBLIC CLOUD ZIEHT AN

Aufgrund der vielen Vorteile, welche die Cloud hinsichtlich Digitalisierung und Security bietet, entscheidet sich laut Lünendonk®-Studie 2020 „Der Markt für IT-Beratung und IT-Service in Deutschland" eine überwiegende Zahl von Unternehmen dazu, künftig einen großen Teil ihrer IT-Anwendungen in die Cloud zu überführen. Vor allem betriebliche Standardsoftware wird zunehmend in die Cloud migriert. Individualanwendungen, die in der Regel komplexe Code-Strukturen haben und sehr stark auf die Unternehmensprozesse angepasst wurden, verbleiben dagegen in 47 Prozent der Unternehmen vorerst im klassischen Rechenzentrumsbetrieb.

Hinsichtlich der Cloud-Bereitstellungsmodelle entscheiden sich 30 Prozent der befragten Unternehmen für eine Verlagerung der überwiegenden Zahl ihrer IT-Anwendungen in die Public Cloud. Dabei wird es sich jedoch in den meisten Fällen um eher geschäftsunkritische Teile von Anwendungen handeln, wohingegen geschäftskritische Workloads in Private Cloud-Umgebungen migriert werden oder im On-Premise-Betrieb verbleiben. Beispiele für geschäftskritische Workloads sind Prozesse, in denen sensible Kundendaten oder Controlling-Informationen verwaltet werden.

Als Konsequenz der zunehmenden Trennung von Geschäftsprozessen und dem Betrieb von Anwendungen über mehrere Betreibermodelle hinweg entstehen hybride Umgebungen, die sehr spezielle Anforderungen an die Orchestrierung, Steuerung und IT-Security-Governance stellen. Immer mehr Unternehmen setzen daher auf sogenannte Managed Cloud Service Provider, die sich um das Management der IT-Umgebungen kümmern und die Schnittstelle zu den Cloud-Providern bilden.

CLOUD-MIGRATION ERHÖHT DEN FOKUS AUF COMPLIANCE UND IT-SECURITY

Wann immer mehr Geschäftsprozesse in der Cloud abgebildet, automatisiert und miteinander zu einer End-to-End-Sicht vernetzt werden (z. B. durch den Digital Twin oder Machine-to-Machine-Kommunikation), ergeben sich in der Konsequenz neue Angriffspunkte für Hacker und Malware, ebenso steigt das Risiko durch Phishing-Mails/CxO Fraud. Tatsächlich gehören höhere Anforderungen an die IT-Sicherheit im Sinne von Zero Trust und an die Einhaltung von Compliance-Richtlinien zu den wichtigsten Herausforderungen bei einer Migration von IT-Anwendungen in die Cloud.

Laut der Lünendonk®-Studie 2019 „Fit für die digitale Transformation" sehen sieben von zehn befragten CIOs und andere IT-Manager beide Themen als eine ihrer größten Herausforderungen. Bestätigung kommt durch eine aktuelle Studie des IT-Branchenverbandes Bitkom (Cloud-Monitor), laut der vier von zehn Unternehmen über Schwierigkeiten bei der Integration von Public-Cloud-Lösungen in die bestehende IT-Infrastruktur berichten.

UNTERNEHMEN GEHEN DEN KONSEQUENTEN WEG IN DIE CLOUD – PUBLIC CLOUD IST KEIN „NO GO" MEHR

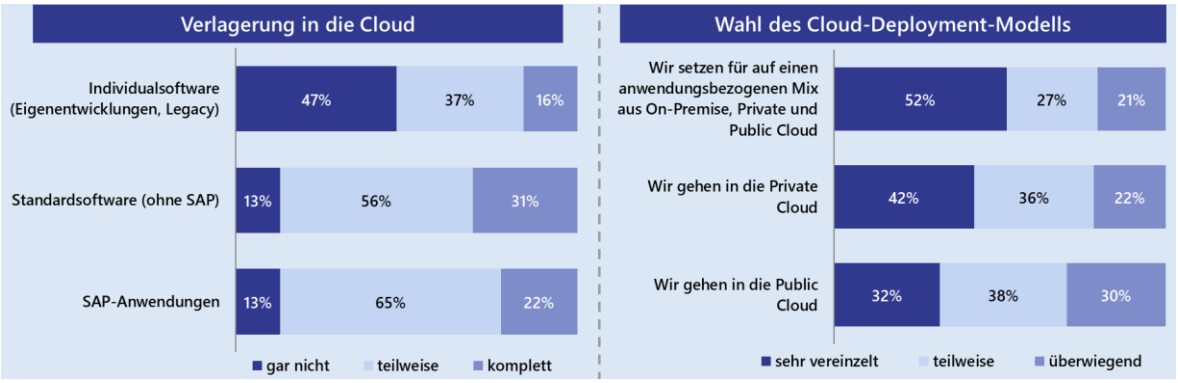


Abbildung 5: Frage: Welche der folgenden IT-Anwendungen verlagern Sie in die Cloud? Mögliche Antworten: „komplett", „teilweise" oder „gar nicht"; n = 153; Frage: Welche Cloud-Deployment-Modelle nutzt Ihr Unternehmen bei der Migration von IT-Alt-Software in die Cloud? Mögliche Antworten: „überwiegend", „teilweise", „sehr vereinzelt"; n = 147; Quelle: Lünendonk®-Studie 2020 „Der Markt für IT-Dienstleistungen in Deutschland"

STEIGENDE IT-SECURITY- UND COMPLIANCE-ANFORDERUNGEN MÜSSEN BEI DER CLOUD-MIGRATION BERÜCKSICHTIGT WERDEN

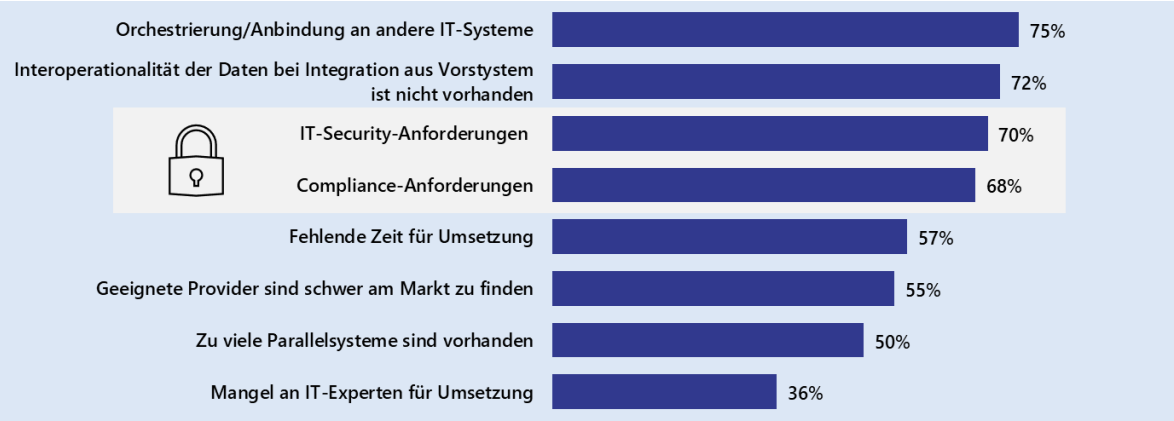


Abbildung 6: Frage: Welche Herausforderungen ergeben sich bei der Cloud-Migration? n = 117; Quelle: Lünendonk®-Studie 2019 „Digitale Transformation – Status quo und Ziele bei der Legacy-Modernisierung und der Cloud Migration"

Große Befürchtungen bestehen der Bitkom-Studie zufolge vor allem bei einem unberechtigten Zugriff auf sensible Unternehmensdaten und auf die Integration von Public Cloud-Lösungen in die bestehenden IT-Architekturen und Sicherheitskonzepte. Allerdings – und dies bestätigt den Trend zur Verlagerung von IT-Anwendungen in die Public Cloud – berichten die Teilnehmer der BITKOM-Studie auch von deutlich weniger IT-Sicherheitsvorfällen in den genutzten Public Cloud-Anwendungen gegenüber den unternehmenseigenen IT-Systemen.

CORONA ALS TREIBER FÜR DEN DIGITAL WORKPLACE UND DAMIT FÜR NEUE SICHERHEITSLÜCKEN

Neben der Verlagerung von IT-Legacy-Anwendungen in die Cloud sind Collaboration-Tools laut der Lünendonk®-Studie 2020 „Der Markt für IT-Beratung und IT-Service in Deutschland" ein weiteres wichtiges Technologiefeld im Jahr 2020, für das hohe Investitionen vorgesehen sind (siehe Abbildung 6). 42 Prozent der Studienteilnehmer werden in diesen Teilaspekt des Digital Workplace sehr stark bis stark investieren.

Vor allem die Covid-19-Krise hat den Durchbruch für den digitalen Arbeitsplatz gebracht und Collaboration-Tools wie Microsoft 365, Teamviewer oder Zoom einen massiven Schub gegeben – aber auch zu ganz neuen Anforderungen und einem Handlungsdruck hinsichtlich Endpoint-Security geführt. Da auf geschäftskritische Anwendungen wie ERP, CRM oder PLM nun in großem Umfang von externen Umgebungen aus zugegriffen wird, müssen cloudbasierte Collaboration-Tools und die sich in Business-Nutzung befindlichen (mobilen) Endgeräte noch stärker in die IT- und Security-Architektur integriert werden.

ERP-MODERNISIERUNG FÜHRT IN DIE CLOUD

Fast jedes vierte (24 %) Unternehmen möchte sehr starke Investitionen in die Modernisierung der ERP-Landschaft vornehmen, weitere 28 Prozent wollen eher stark investieren. Dabei geht es im deutschsprachigen Raum vor allem in Großunternehmen und Konzernen um die ERP-Lösungen von SAP und Microsoft. Beide Anbieter machen etwa die Hälfte des ERP-Marktes aus und haben eine klare Cloud-First-Strategie.

Laut der 2019 veröffentlichten Lünendonk®-Studie „Mit S/4HANA in die digitale Zukunft" plante jedes zweite Unternehmen die S/4HANA-Anwendungen entweder komplett in der Cloud oder in hybriden Umgebungen laufen zu lassen.

DIE TOP-INVESTITIONSTHEMEN FÜR 2020–2021

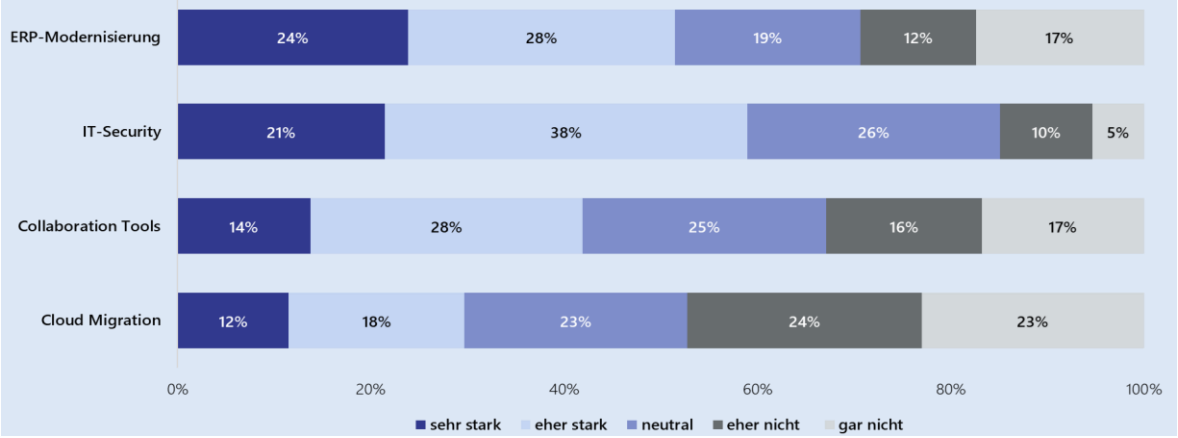


Abbildung 7: Frage: In welche konkreten Technologien investiert Ihr Unternehmen in diesem Jahr? Skala von –2 = „gar nicht" bis +2 = „sehr stark"; Häufigkeitsverteilung; n=168; Quelle: Lünendonk®-Studie „Der Markt für IT-Dienstleistungen in Deutschland", 2020

Gründe für den immer häufiger bevorzugten Betrieb des sogenannten Digital Core – vor allem der ERP - in der Cloud sind die höhere Entwicklungs- und Deployment-Geschwindigkeit neuer Software und Releases sowie die bessere Möglichkeit bei plattformbasierten Geschäftsmodellen, Third-Party-Lösungen anzubinden. Dadurch ergeben sich aber auch neue Anforderungen an das IT-Risikomanagement und die Steuerung der Sourcing-Modelle. So müssen geschäftskritische Anwendungen (ERP, PLM) häufig auf Multi-Cloud-Plattformen betrieben werden, um von vornherein die Geschäftsprozesse auf mehrere Hyperscaler und andere Cloud-Anbieter zu verteilen. Damit soll im Rahmen von Business-Continuity-Management-Strategien sichergestellt werden, dass ein Shift von einer Cloud-Plattform auf die andere in kurzer Zeit möglich ist – für den Fall, dass beispielsweise ein Cloud-Anbieter einen bestimmten Cloud-Service abschaltet oder ein Service ausfällt.

HÖHERE IT-SICHERHEITSANFORDERUNGEN FÜHREN ZU HÖHEREN IT-BUDGETS

Ein Blick auf die geplanten IT-Budgets für 2021 verdeutlicht die steigenden Anforderungen aus der zunehmenden Cloud-Nutzung. Der Wandel zum stärkeren Bezug von Cloud-Services geht einher mit einer Neuausrichtung der IT-Architektur, also des Bebauungsplans für die IT-Landschaft. So sind beispielsweise Aspekte wie Schnittstellenoffenheit, Modularität, Skalierbarkeit, Datensicherheit und Cyber Security bei einer Cloud-Architektur deutlich höher priorisiert.

Damit sensible Geschäfts- oder Kundendaten auch in Cloud-Umgebungen kontinuierlich vor unbefugten externen Zugriffen geschützt sind, liegt laut Lünendonk®-Studie 2020 „Der Markt für IT-Beratung und IT-Service in Deutschland" ein Investitionsschwerpunkt auf dem Thema IT-Security. Konkret wollen 59 Prozent der Studienteilnehmer 2020 sehr stark oder eher stark in Technologien zur Cyber-Abwehr investieren. Besonders hoch ist der Anteil derjenigen Unternehmen, die einen Investitionsschwerpunkt auf IT-Security-Technologien legen, bei den Banken und Logistikunternehmen (je 73 %). Aber auch im Energiesektor (58 %), im Handel (65 %) und in der Industrie (57 %) plant jeweils die Mehrheit der befragten Unternehmen mit höheren Ausgaben für die IT-Sicherheit.

Die höhere Priorisierung der IT-Sicherheit wird auch durch die geplanten Entwicklungen der IT-Budgets für das Jahr 2021 in großen Unternehmen deutlich: Tatsächlich werden es laut Lünendonk®-Studie 2020 „Der Markt für IT-Beratung und IT-Service in Deutschland" nur 2 Prozent der Unternehmen 2021 ihre IT-Security-Budgets reduzieren, während 42 Prozent ihre Ausgaben für IT-Sicherheit erhöhen werden (Abbildung 7).

MEHR AUFLAGEN AN DIE CLOUD-GOVERNANCE ERHÖHEN DIE KOSTEN FÜR DEN IT-BETRIEB

Trotz der Zunahme an Cloud-Bereitstellungsmodelle werden nur die wenigsten Unternehmen ihre Budgets für den IT-Betrieb reduzieren: Während 57 Prozent von konstanten Ausgaben für den IT-Betrieb ausgehen, planen weitere 24 Prozent höhere IT-Betriebsausgaben ein.

Diese Entwicklung hängt damit zusammen, dass mit der intensiveren Cloud-Nutzung – vor allem der Public Cloud – höhere Anforderungen seitens der Aufsichtsbehörden sowie der eigenen Compliance-Regeln an die Nutzung von Cloud-Diensten einhergehen. So gelten in stark regulierten Branchen wie Energie, Finanzdienstleistungen und Telekommunikation besondere Auflagen seitens der Aufsichtsbehörden – beispielsweise im Hinblick auf sicherheitsrelevante Aspekte wie Daten- und Informationssicherheit, Datenhoheit, Zugriffsrechte und ganz besonders den Schutz der Kernanwendungen vor Hackerangriffen.

Auch in anderen Kernbranchen wie Automotive und dem Maschinenbau gelten besonders hohe Anforderungen an den Schutz geistigen Eigentums oder vor Produktpiraterie – beispielsweise durch den Diebstahl von Patenten für Innovationen oder von Entwicklungsplänen für Produkte. Aber auch Erpressungen durch Lösegeldforderungen nehmen in der Wirtschaftskriminalität stark zu, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelmäßig feststellt.

BUDGETENTWICKLUNG NACH EINZELNEN THEMEN IN ANWENDERUNTERNEHMEN

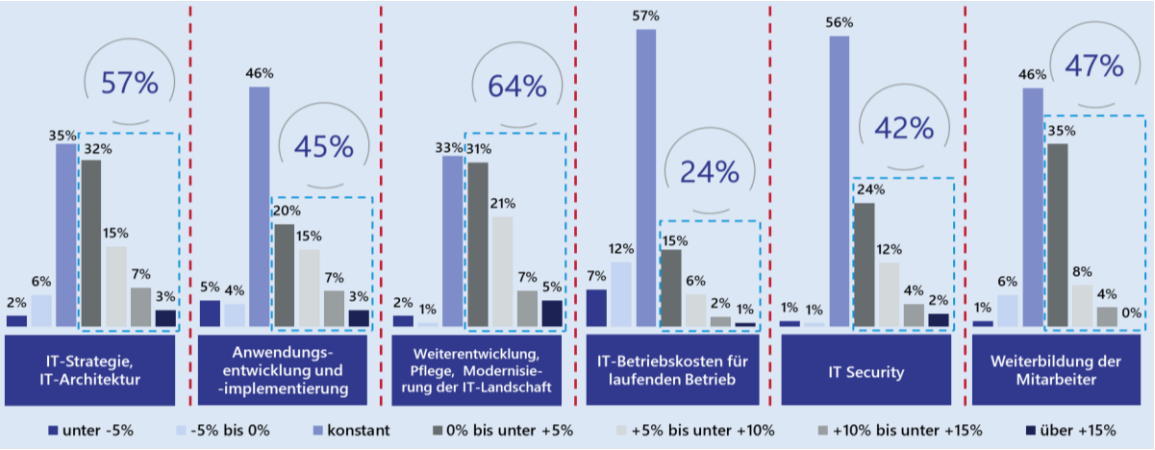


Abbildung 8: Frage: Wie werden sich Ihre IT-Budgets von 2020 auf 2021 entwickeln (Inklusive interner und externer Ausgaben)? Häufigkeitsverteilung; n = 162; Quelle: Lünendonk®-Studie „Der Markt für IT-Dienstleistungen in Deutschland", 2020

Cyber Security gehört auf die CxO-Agenda

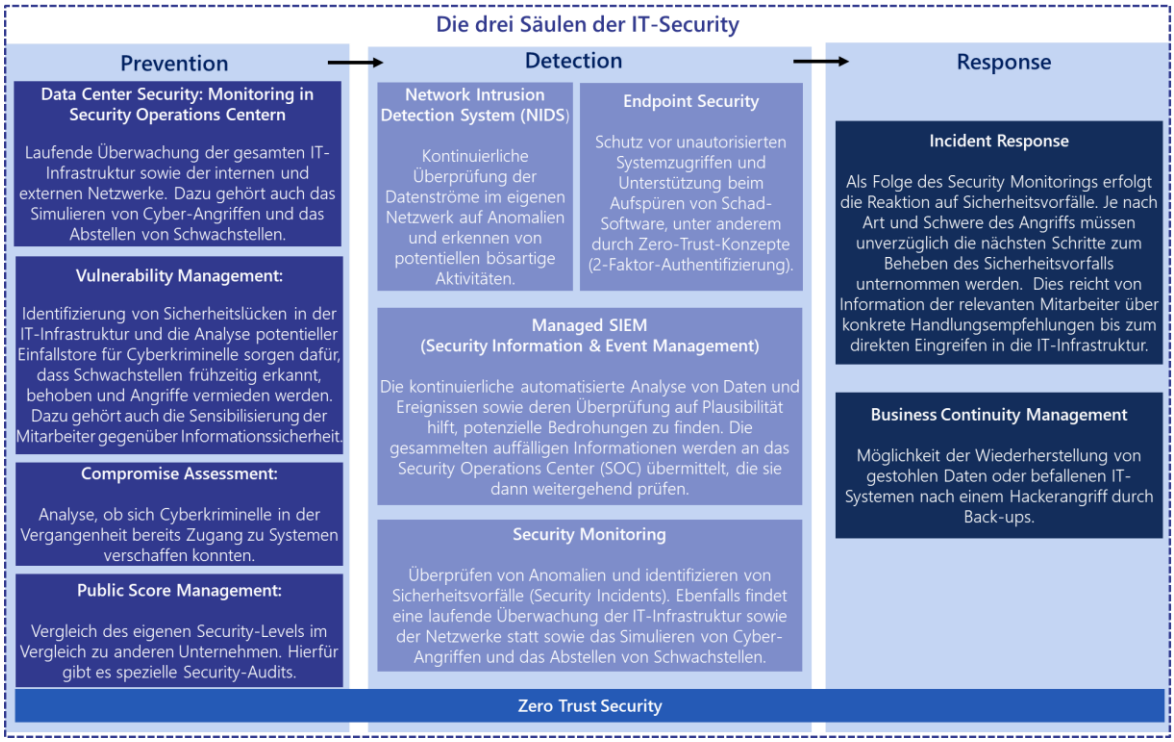


Abbildung 9: Kernbestandteile der Cyber Security; Quelle: Lünendonk

Die steigenden Investitionen in die Cyber-Abwehr sind im Zuge der digitalen Transformation und der nahezu vollständigen Digitalisierung von Prozessen und Informationen absolut notwendig. Cyber-Angriffe werden seit Jahren stetig professioneller und richten sich zunehmend auf unternehmenskritische Prozesse. Erschwerend kommt für die Cyber-Abwehr hinzu, dass die Zahl bekannter Schadsoftware-Varianten seit 2011 jedes Jahr um 40 Prozent gestiegen ist (Quelle: AVTest). Besonders stark von Cyber-Angriffen betroffen sind die Windows-Plattformen, wobei sich die Zahl der Malware-Varianten für das Android-Betriebssystem in den letzten Jahren ebenfalls enorm erhöht hat. Aber auch IoT-Betriebssysteme wie Linux und Unix verzeichnen laut AVTest seit 2018 exponentiell wachsende Malware-Angriffe.

Um ein Beispiel für die Dimensionen zu geben: Allein auf die IT-Infrastruktur der Deutschen Telekom erfolgen 71 Millionen Angriffe – pro Tag. Allein in den Jahren 2018 und 2019 verzeichnete das Bundesamt für Sicherheit in der Informationstechnik (BSI) 114 Millionen neue Schadprogramm-Varianten, mit denen Cyber-Kriminelle IT-Infrastrukturen und Netzwerke kontinuierlich und zunehmend automatisiert mithilfe von Bots angreifen.

Laut dem BSI werden Cyber-Angriffe vor allem durch die folgenden Schwachstellen in Unternehmensinfrastrukturen ermöglicht:

- SOFTWARE-SCHWACHSTELLEN: Häufig bieten Programmierfehler Angriffsflächen für Cyber-Kriminelle. Da der Quellcode größerer Software-Produkte mehrere Millionen Programmierzeilen lang sein kann, sind solche Software-Schwachstellen nicht selten. Aber auch veraltete Software ist ein häufiges Problem, da in vielen Unternehmen die IT-Landschaft

über Jahrzehnte gewachsen und durch einen hohen Anteil von Individualsoftware geprägt ist.

- DESIGN-SCHWACHSTELLEN: Legacy-IT weist neben veralteten Codes vor allem Mängel im Design auf. So mangelt es oft an der Spezifikation von Zugriffsrechten, Schnittstellen, Datenformaten und Übertragungsprotokollen.

- KONFIGURATIONSSCHWACHSTELLEN: Die Implementierung von Software und IT-Systemen ist eine weitere Schwachstelle. Beispielsweise können bei der Implementierung bestimmte Sicherheitsfunktionen deaktiviert oder Zugriffsrechte nicht restriktiv genug konfiguriert werden.

- MENSCHLICHE FEHLHANDLUNGEN: Täter verwenden vielfältige Tricks, um Mitarbeiter zur Mithilfe bei Cyber-Angriffen zu bewegen („Social Engineering"). Durch täuschend echte Phishing-Mails werden Mitarbeiter und Führungskräfte dazu bewegt, eine E-Mail zu öffnen und auf bestimmte Schaltflächen zu klicken. Die dahinter liegenden Webseiten sehen zunehmend täuschend echt aus, sodass die Mitarbeiter keinen Verdacht schöpfen.

ELEMENTE EINER CYBER-SECURITY-STRATEGIE

Abbildung 6 zeigt aus Sicht von Lünendonk einige Kernelemente zum Schutz vor Cyber-Angriffen. Ein ganz wesentlicher Punkt – der in vielen Unternehmen zu einem Mentalitätswandel führen muss – ist, dass Cyber Security in Zeiten von Digitalisierung und plattformbasierten Geschäftsmodellen nicht mehr nur die IT-Infrastrukturebene betrifft, sondern vor allem den Schutz der Geschäftsprozesse, des geistigen Eigentums und anderer sensibler Unternehmensdaten.

DAS RISIKO KENNEN UND BEURTEILEN KÖNNEN

Es gilt daher in der digitalen Welt, Cyber Security als integralen Teil des Compliance- und Risikomanagements zu betrachten und stärker in den Fokus zu rücken. Ein häufig auftretendes Problem im Risikomanagement besteht allerdings darin, das monetäre Risiko von Cyber-Angriffen zu bewerten und die Maßnahmen entsprechend der Risikobeurteilung vorzunehmen. Nicht selten sind Cyber-Angriffe und Datendiebstahl gar nicht bekannt – unter anderem weil die Monitoring-Systeme nicht auf die neuen Bedrohungen ausgelegt sind und Angriffe nicht erkannt oder gemeldet werden.

Ein kontinuierliches Monitoring des gesamten Unternehmensökosystems (Unternehmensinfrastruktur, mobile Endgeräte, Third-Party-Anwendungen) in sogenannten Security Operations Centers (SOCs) hilft grundsätzlich, die Bedrohungslage einzuschätzen. Im SOC sollten Security-Spezialisten organisatorisch angesiedelt sein, um daraus eine eigene Einheit zu schaffen und den Experten die Möglichkeit zu geben, sich komplett auf die Cyber-Abwehr zu konzentrieren. SOCs sind oft losgelöst von anderen IT-Teams, um unabhängiger von der IT zu sein. SOCs Sie müssen aber nicht unbedingt innerhalb eines Unternehmens angesiedelt sein, sondern können auch an Dienstleister für IT-Security ausgelagert werden (Managed Security Services). So fehlen in vielen Unternehmen Security-Experten für den Aufbau von SOCs.

„SCHWACHSTELLE" MITARBEITER

Eine weitere wichtige Voraussetzung für den Schutz vor Cyber-Angriffen ist die Abgrenzung zwischen Social Engineering und echtem Hacking. Während beim Social Engineering eine Benutzeraktion erforderlich ist, laufen Hackerangriffe in der Regel automatisiert über Bot-Farmen. Laut Microsoft Security Report erfolgen 71 Prozent der Cyber-Angriffe durch Social Engineering und 29 Prozent über echtes Hacking. Beim Social Engineering werden Mitarbeiter vor allem durch Phishing-Mails dazu gebracht, auf Schadsoftware enthaltende Webseiten zu navigieren. Die Methoden der Angreifer sind mittlerweile sehr ausgereift. Sowohl die Phishing-Mails als auch die (Fake-)Internetseiten sind rein optisch kaum von den Originalseiten zu unterscheiden und verleiten den Nutzer dazu, Identitätsdaten preiszugeben. Um diese Seriosität weiter zu untermauern, setzen Angreifer bei den erstellten

Phishing-Seiten vermehrt auf das Secure Hypertext Transfer Protocol (HTTPS), das für eine abhörsichere und nicht manipulierbare Datenübertragung steht und durch „einfache" Anti-Viren-Programme nicht erkannt wird. Die kontinuierliche Sensibilisierung der Belegschaft zur Informationssicherheit in Form von Schulungen, Workshops und gesteuerten Phishing-Tests ist ein wichtiges Instrument in der IT-Sicherheit.

INCIDENT RESPONSE UND BUSINESS CONTINUITY MANAGEMENT

Wenn Cyber-Angriffe nicht abgewehrt werden konnten, gilt es, im Rahmen der Incident Response sehr schnell Maßnahmen zu ergreifen. Eine wichtige Rolle kommt dabei dem Business Continuity Management zu, worunter Strategien, Pläne, Maßnahmen und Prozesse zu verstehen sind, um Schäden durch die Unterbrechung des IT-Betriebs in einem Unternehmen oder einer Organisation zu minimieren.

Notfallkonzepte im Falle von Hackerangriffen und Malware-Infizierung sollten vor allem die schnelle Wiederherstellung der IT-Systeme und Datenbanken durch Back-ups und die Trennung von mobilen Endgeräten und externen Quellen von der Unternehmensinfrastruktur gewährleisten.

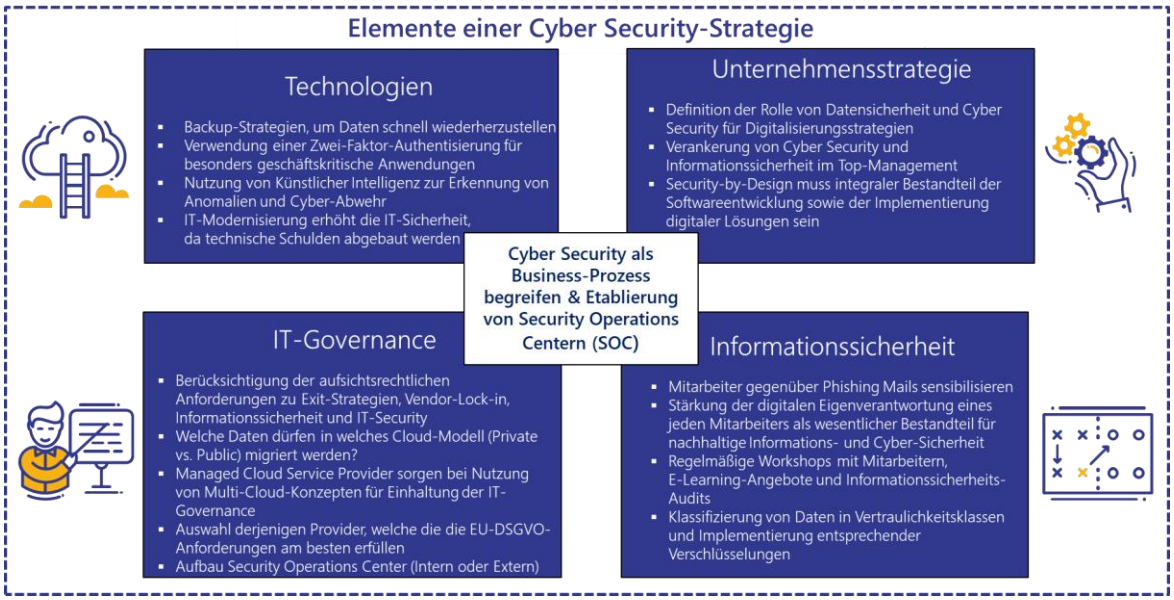


Abbildung 10: Elemente einer Cyber Security-Strategie; Quelle: Lünendonk

Security-Risiken erkennen – am besten bevor sie auftreten

SECURITY OPERATIONS CENTER

Die Fülle an Aufgaben sowie der Druck zur Cyber-Abwehr sind groß. Immer mehr Unternehmen setzen auf sogenannte Security Operations Centers (SOCs). Dabei handelt es sich um eigene Organisationseinheiten, die für die kontinuierliche Überwachung der IT-Systeme und für die Informationssicherheit verantwortlich sind. SOCs können sowohl intern als auch extern oder als hybride Formen – abhängig von der Verfügbarkeit von Inhouse-Security-Experten – betrieben werden.

SOCs beschäftigen sich vor allem mit der Prävention, dem aktiven Schutz, der Erkennung und dem Behandeln von Cyber-Angriffen. Dabei werden Ansätze und Technologien wie Schwachstellenmanagement, Gefährdungsbewertung und Endpoint Detection, Security Monitoring oder SIEM-Systeme (Security Information and Event Management) in einem zentralen Center of Excellence gebündelt. Dieser Ansatz verspricht die bestmögliche Umsetzung von Sicherheitskonzepten durch Kombination aller relevanten Aufgaben in einer zentralen Organisation und den Wegfall von Schnittstellen und damit verbundenen Abstimmungsproblemen.

Ein sehr wichtiger Mehrwert eines SOC ergibt sich aus dem IT-Risikomanagement. Insbesondere stark regulierte Branchen (Banken, Versicherungen, Energieversorger, Healthcare), aber auch zunehmend Unternehmen anderer Branchen müssen Prüfungs-Audits zu den von den Aufsichtsbehörden oder eigenen Governance-Regeln geforderten Sicherheitsstandards durchführen. Da im SOC alle sicherheitsrelevanten Ereignisse und Maßnahmen dokumentiert werden, lassen sich die notwendigen Kennzahlen vergleichsweise einfach erheben und reporten. In der Regel erstellt das SOC kontinuierlich Security-Reports zu den relevanten Kennzahlen. Sofern das SOC an einen externen IT-Dienstleister ausgelagert ist, sind auf der Basis des SOC-Reportings vertraglich geforderte Security Service Levels unmittelbar verfügbar und nachweisbar.

DIE AUFGABEN EINES SECURITY OPERATIONS CENTER

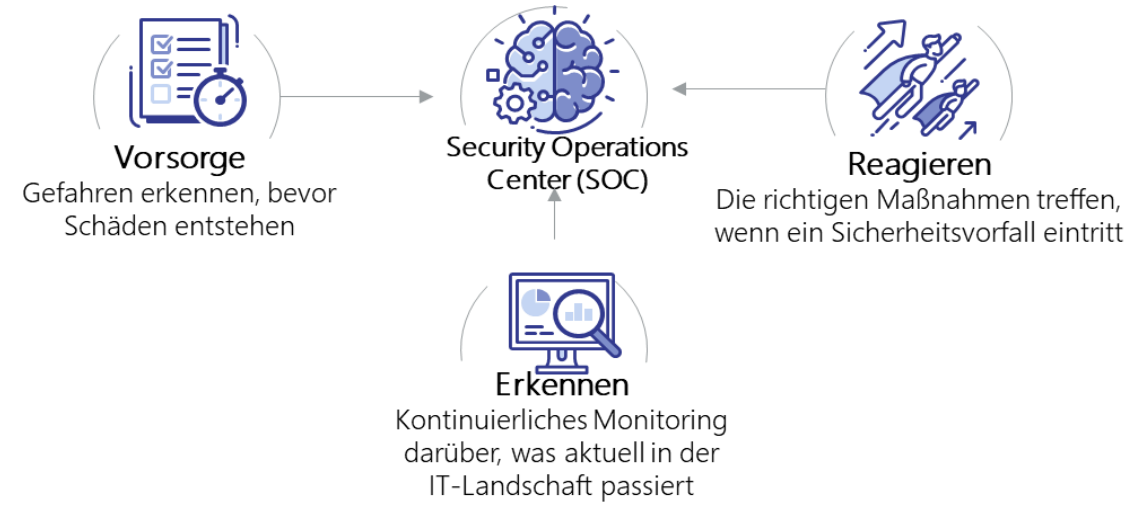


Abbildung 11: Aufgaben eines Security Operations Center; Quelle: Lünendonk

KÜNSTLICHE INTELLIGENZ

Die Aufgaben, die für den Schutz vor Cyber-Angriffen notwendig sind, werden im Zuge der Digitalisierung immer vielfältiger und komplexer. So gilt es für ein SOC nicht nur, die eigene IT-Infrastruktur kontinuierlich zu tracken, sondern das gesamte Ökosystem, bestehend aus IoT-Netzwerken oder Third-Party-Anwendungen bei E-Commerce-Portalen. Aus dem höheren Digitalisierungsgrad heraus entstehen enorme Mengen an Log-Daten und unzählige Angriffsmuster, die verarbeitet werden müssen – idealerweise in Echtzeit, da beispielsweise Malware sehr schnell großen Schaden anrichten kann und entsprechend schnell reagiert werden muss, um lange Systemausfälle zu vermeiden. Die steigende Datenmenge und die Komplexität im Cyber-Security-Tracking stellen viele Security-Abteilungen aber vor große Herausforderungen, die Flut an Gefahren zu erkennen und abzuwehren. Das führt dazu, dass Unternehmen in Zeiten der Digitalisierung eine deutlich höhere Zahl von Schwachstellen haben als in der Vergangenheit.

Um die steigende Datenflut in den Griff zu bekommen, aber auch um die Security-Experten von aufwendigen Routineaufgaben zu entlasten, denken Unternehmen immer häufiger über den Einsatz künstlicher Intelligenz beziehungsweise Machine Learning bei der Cyber Security nach. Die kontinuierliche und automatisierte Analyse von Daten und Ereignissen sowie deren Überprüfung auf Sinnhaftigkeit hilft den Mitarbeitern im SOC, potenzielle Bedrohungen frühzeitig zu erkennen, zu klassifizieren und gegebenenfalls auf die Angriffe schnell zu reagieren.

Das große Problem für Unternehmen ist die hohe Geschwindigkeit, mit der Cyber-Kriminelle neue Malware, Ransomware und Bot-Netzwerke erstellen. Allein im Jahr 2019 wurden laut BSI täglich bis zu 110.000 Bot-Infektionen deutscher Systeme registriert. Bei Malware wurden etwa 114 Millionen neue Varianten ermittelt und auch bei Ransomware ist ein starker Anstieg zu verzeichnen. Grundsätzlich sind die Cyber-Angreifer den meisten Unternehmen deutlich überlegen – vor allem weil sie technologisch im Vorteil sind. Gerade für mittelständische Unternehmen ist es sehr schwer, mit der technologischen Entwicklung Schritt zu halten und die notwendigen Security-Fachkräfte zu rekrutieren.

Auf Machine Learning basierte Algorithmen haben den Vorteil, kontinuierlich und automatisiert Millionen von Ereignissen zu überwachen. Muster (Anomalien) lassen sich so schneller erkennen. Vor allem um der steigenden Zahl von Bot-Angriffen etwas entgegenzusetzen, lohnt es sich, sich mit Machine Learning zu befassen und auch KI-betriebene Bots einzuführen, die die Netzwerke nach Gefahren tracken. Der große Vorteil von KI-basierten Security Services ist, dass KI-Technologien die IT-Netzwerke in einem 24×7-Modus tracken können und damit eine Reihe von Angriffspunkten schließen. Allerdings ist für den Einsatz von KI in den SOCs ausgeprägtes Know-how notwendig, beispielsweise um KI-Modelle zu entwickeln und die Machine Learning Engines zu trainieren. KI-Experten sind jedoch – genau wie Security-Experten – am Markt sehr knapp verfügbar, weshalb Unternehmen immer häufiger Teile ihrer SOCs in die Verantwortung externer Dienstleister (Managed Security Service Partner) übergeben.

EINSATZ VON KÜNSTLICHER INTELLIGENZ ZUR ERHÖHUNG DER CYBER SECURITY

Abbildung 12: Einsatzformen künstlicher Intelligenz in der IT-Security; Zusammenstellung durch Lünendonk

Intern oder extern? Der Bedarf an Managed Security Services nimmt zu

IT-Security-Strategien stehen und fallen mit dem Erfolg ihrer Umsetzung – also der tatsächlichen Operationalisierung. Dabei kommt es, neben der passenden Security-Strategie und den technologischen und organisatorischen Voraussetzungen – vor allem auf die Verfügbarkeit von Security-Experten an, um die Security-Konzepte auch wirksam umzusetzen. Allerdings mangelt es genau an diesem Punkt an Fachkräften.

Betrachtet man die für den Umbau der IT-Landschaften benötigten Qualifikationen, werden laut der Lünendonk®-Studie „Fit für die digitale Transformation – Status quo und Ziele bei der Legacy-Modernisierung und der Cloud Migration" in 56 Prozent der befragten großen mittelständischen Unternehmen und Konzerne vor allem IT-Security-Experten benötigt. Dass in Zeiten des Fachkräftemangels nicht alle offenen Stellen besetzt werden können, liegt auf der Hand. Vor allem mittelständische Unternehmen, aber auch große Konzerne tun sich bei der Rekrutierung von IT-Spezialisten aus unterschiedlichen Disziplinen schwer: Laut der Lünendonk®-Studie 2020 „Der Markt für IT-Dienstleistungen in Deutschland" haben 37 Prozent der Unternehmen im IT-Security-Management keine ausreichende interne Expertise.

BEDARF AN END-TO-END-SERVICES STEIGT

Wie das zweite Kapitel gezeigt hat, plant eine große Mehrheit der Unternehmen die Migration ihrer IT-Systeme und -Infrastrukturen in die Cloud. Dabei spielt die Bereitstellung von Workloads und IT-Services aus der Public Cloud eine immer wichtigere Rolle.

Es gilt jedoch, eine Fülle an fachlichen, technologischen und regulatorischen Anforderungen zu beachten. Komplexe Aufgaben sind unter anderem die folgenden:

- Trennung von Geschäftsprozessen in kritische und unkritische Systeme
- Betrieb von Workloads, IT-Services und Geschäftsprozessen über mehrere Betreibermodelle (Public- und Private Cloud, On-Premise)
- Kontinuierliches Monitoring der (regulatorischen) Governance-Anforderungen im Hinblick auf Themen wie IT-Sicherheit, Datenschutz und Datensouveränität
- Ermöglichen von Security-Audits durch Aufsichtsbehörden und Wirtschaftsprüfer

IT-SECURITY-EXPERTEN SIND GEFRAGT – ABER AUCH SCHWER AM MARKT VERFÜGBAR

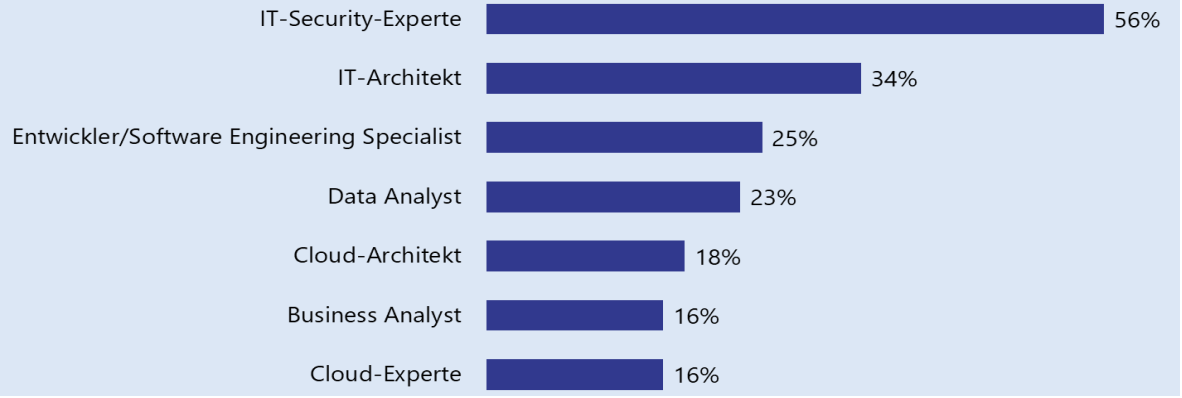


Abbildung 13: Frage: Für die Weiterentwicklung der IT-Infrastruktur und die damit einhergehende Veränderung der Organisationsstrukturen werden neue Qualifikationen benötigt. Welche drei Rollenprofile benötigen Sie derzeit am häufigsten? n = 117; Quelle: Lünendonk®-Studie 2019 „Fit für die digitale Transformation – Status quo und Ziele bei der Legacy-Modernisierung und der Cloud Migration"

Die künftigen IT-Landschaften werden durch hybride Bereitstellungsmodelle – also einen Mix aus On-Premise, Public und Private Cloud – geprägt sein. Daraus ergeben sich aus Sicht von Lünendonk einige neue Anforderungen an das Management und die Steuerung hybrider IT-Umgebungen:

- Sicherstellung der Integrationsfähigkeit der bestehenden Anwendungen in die Cloud über APIs
- Vernetzung der unterschiedlichen Betreibermodelle (Orchestrierung) durch Schnittstellen/APIs
- Sicherstellung der Data Privacy/Datenhoheit
- Management der Cloud Governance
- Erfüllung der regulatorischen Anforderungen hinsichtlich Datensicherheit und Cyber-Risiken
- Monitoring der Cloud-Netzwerke hinsichtlich IT-Security-Risiken
- Kostenkontrolle und Abrechnungen mit den Cloud-Providern
- Schutz vor Abhängigkeiten von Cloud-Anbietern

Im Zuge von mehr unternehmensübergreifender Vernetzung ist ein weiterer Einflussfaktor für steigende Security-Anforderungen der Trend zur Entwicklung von Cloud-native-Softwarelösungen und APIs. Bereits beim Design digitaler Produkte und Schnittstellen ist es wichtig, die notwendigen Sicherheitsanforderungen zu berücksichtigen (Security by Design), die gelten müssen, wenn im Rahmen digitaler Geschäftsmodelle sensible Kundendaten gesammelt werden.

MANAGED CLOUD SERVICE PROVIDER

Aufgrund der Vielzahl von Aufgaben und eines gleichzeitigen Mangels an Inhouse-Expertise ist am Markt zu beobachten, dass immer mehr Unternehmen auf sogenannte Managed Cloud Service Provider setzen. Gerade wenn es um den Betrieb von Geschäftsprozessen auf mehreren Clouds (Multi-Cloud) geht, bevorzugen immer mehr Unternehmen einen Dienstleister, der als eine Art Broker zwischen Cloud-Anbieter und Kunden steht.

Das Nachfragebarometer von Lünendonk für den deutschen IT-Dienstleistungsmarkt bestätigt diese Entwicklung: Eine große Mehrheit der in Deutschland führenden IT-Dienstleister hatte bereits im Jahr 2019 eine große Nachfrage ihrer Kunden nach Cloud-Transformation, IT-Modernisierung und Cyber Security zu verzeichnen. Auch hinsichtlich der Neuausrichtung der IT-Strategien und -Architekturen ist der Bedarf an externer Unterstützung sehr hoch – beispielsweise weil Sicherheitsanforderungen in Architekturkonzepten für IoT-Strategien oder plattformbasierte Geschäftsmodelle berücksichtigt werden müssen.

THEMEN, BEI DENEN DIE FÜHRENDEN IT-DIENSTLEISTER EINE NACHFRAGE DURCH IHRE KUNDEN ERWARTEN

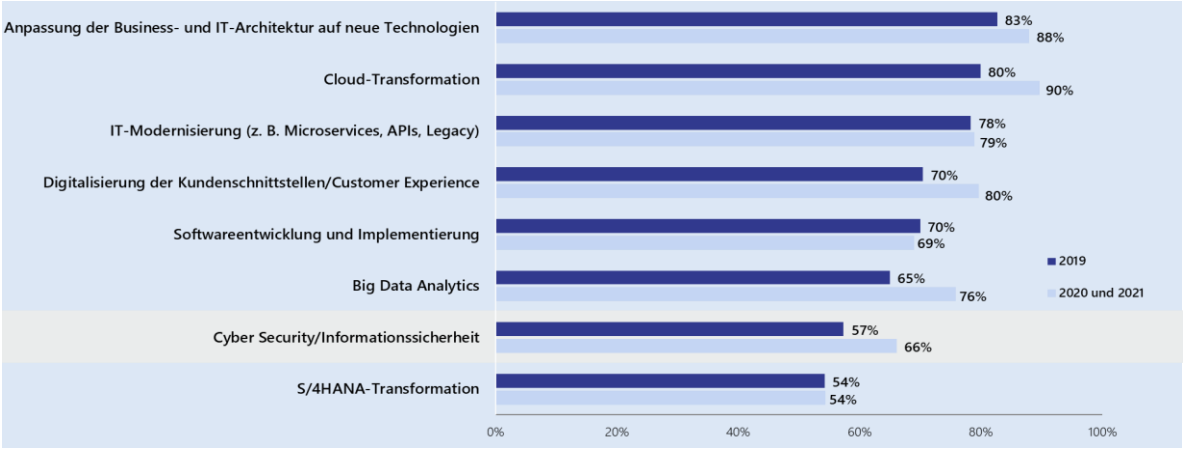


Abbildung 14: Frage: Welche Themen haben 2019 die Nachfrage nach Ihren Services besonders beeinflusst? Skala von –2 =„gar nicht“ bis +2 = „sehr stark“; relative Häufigkeiten; Angaben beziehen sich nur auf die Werte „sehr stark“ und „stark“; Quelle: Lünendonk®-Studie 2020 „Der Markt für IT-Beratung und IT-Service in Deutschland“

Für das Jahr 2020 erwarten die IT-Dienstleister – der steigenden Nachfrage nach Cloud-Angeboten folgend – auch einen höheren Bedarf ihrer Kunden nach externen Security Services. Der Bedarf an Security Services ist im Zuge der weiteren Digitalisierung von Geschäftsmodellen und -prozessen immer höher: So führen neben der Cloud-Transformation auch die Digitalisierung der Kundenschnittstellen und der Aufbau digitaler Kunden-Touchpoints zu einer weiteren Vernetzung von Geschäftsprozessen mit den mobilen Endgeräten der Endkunden. Da viele Endgeräte und Betriebssysteme noch immer nicht optimal geschützt sind beziehungsweise Hacker sich über eine einzelne App über die Smartphones und Tablets von Konsumenten auch Zugang zu Unternehmensnetzwerken verschaffen können, steigt mit zunehmenden digitalen Geschäftsmodellen das Bedrohungspotenzial exponentiell an.

KUNDEN FORDERN END-TO-END-ANSÄTZE

Mit isolierten Security-Ansätzen ist es aufgrund der komplexen Bedrohungslage und der vielschichtigen Herausforderungen rund um die Nutzung von Cloud-Services nicht getan. Der Schutz vor Cyber-Angriffen ist folglich aus Sicht eines großen Teils von CIOs eine Kernanforderung eines Cloud-Dienstleisters. Zwei Drittel der befragten CIOs wünschen sich von IT-Dienstleistern, dass sie im Rahmen von Cloud-Migrationen das gesamte Cloud-Sourcing-Portfolio abdecken – und zudem auch Managed Security Services gehören.

Weiterhin ist es 85 Prozent wichtig, dass das Hosting der Daten in der EU erfolgt, und für besonders sensible Daten bestehen 67 Prozent der Unternehmen auf einem Daten-Hosting in Deutschland. Dieser Forderung kommen die relevanten drei Hyperscaler Amazon Web Services, Microsoft Azure und Google Cloud mittlerweile auch nach und haben in Europa und Deutschland eine Vielzahl von Cloud-Rechenzentren eröffnet.

Aufgrund der teilweise hohen Governance-Anforderungen an die Nutzung der Cloud-Plattformen der Hyperscaler, des Mangels an Inhouse-Experten und der häufig notwendigen Trennung von Geschäfts- und IT-Prozessen auf mehrere Clouds entscheiden sich immer mehr Unternehmen für Managed Cloud Provider, die die technische Betreuung der IT-Landschaften übernehmen. Dabei ist es eine sehr wichtige Anforderung, dass diese Provider auch über umfangreiche Managed Security Services verfügen.

ANFORDERUNGEN AN MANAGED CLOUD PROVIDER

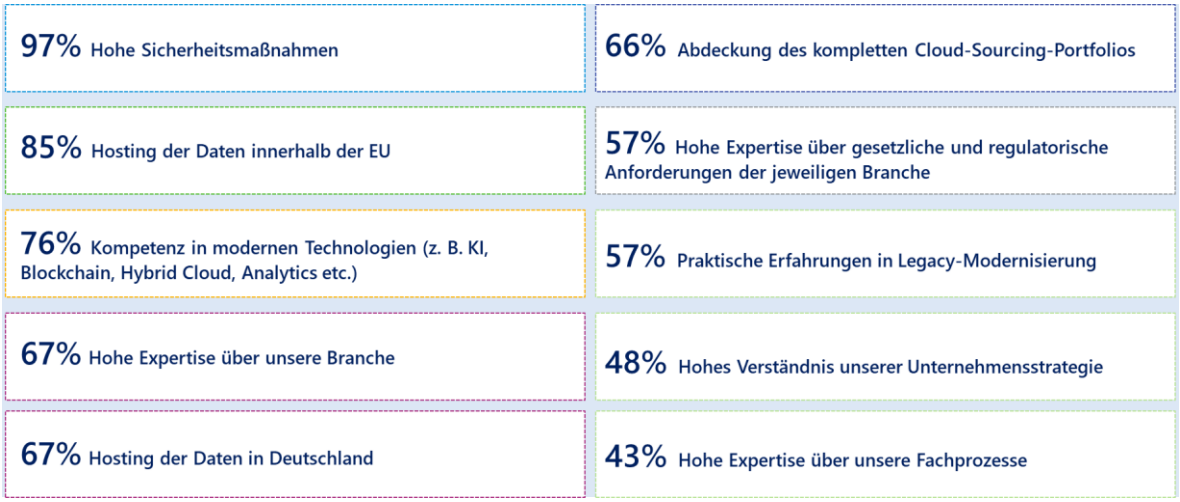


Abbildung 15: Frage: Welche Anforderungen muss ein Managed Cloud Provider erfüllen, damit Sie mit Ihm zusammenarbeiten? n = 122; Quelle: Lünendonk®-Studie „Fit für die digitale Transformation – Status quo und Ziele bei der Legacy-Modernisierung und der Cloud Migration"

Fazit und Ausblick

Cyber Security hat sich in den letzten Jahren aus der IT-Nische zu einem der wichtigsten Digitalthemen entwickelt und erlangt zunehmend Top-Management-Attention. Es ist undenkbar, dass digitale Geschäftsmodelle, die den Schutz von Kundendaten nicht garantieren oder – noch schlimmer – die Gesundheit der Nutzer gefährden, erfolgreich sind. Unternehmen, die Cyber-Bedrohungen ignorieren oder zumindest nicht hoch genug priorisieren, laufen Gefahr, einen immensen Reputationsverlust zu erleiden. Gerade in Zeiten von Social Media und Shitstorms entsteht über Nacht ein negatives Image.

Security by Design, also die Berücksichtigung von Security-Elementen bereits während der Produktentwicklung, ist folglich eine Kernanforderung von digitalen Geschäftsmodellen und deren Akzeptanz am Markt. Die Bedrohungslage ist in jedem Fall vorhanden: Über 100 Milliarden Euro Schaden entstand der deutschen Wirtschaft im Jahr 2019 durch Cyber-Kriminalität – Tendenz im Zuge der fortschreitenden Digitalisierung sicher steigend.

Die digitale Plattformökonomie bietet den Cyber-Kriminellen auch ideale Bedingungen: Haben sie es erst einmal geschafft, in die IT-Systeme zu gelangen, können sie an sensible und vertrauliche Daten gelangen oder ganze Geschäftsprozesse stilllegen. In der Öffentlichkeit werden nur wenige Fälle bekannt – vor allem wenn kritische Infrastrukturen betroffen sind, deren Ausfälle sich nicht verschweigen lassen. Laut dem Bundesamt für Sicherheit in der Informationstechnik ist die Bedrohungslage in jedem Fall enorm und die Täter werden immer einfallsreicher. Das Spektrum der Motive reicht von Industriespionage durch ausländische Regierungen bis hin zur Erpressung und Schutzgeldzahlungen.

Ein Problem für die meisten Unternehmen ist ihre veraltete IT-Landschaft, die enorm viele Angriffspunkte bietet – einfach weil sie technologisch veraltet sind und Hacker sich mit einfachen Tricks Zugang verschaffen können. Technische Schulden, also Programmierfehler oder immer wieder neu angebaute Software-Monolithen, machen die Legacy-IT zu einem unkalkulierbaren Sicherheitsrisiko. Richtig problematisch wird es, wenn im Zuge von Industrie 4.0 die operativen Kernsysteme wie Produktion und Logistik (Operational IT) mit der IT-Infrastruktur vernetzt werden. Das richtige Schlupfloch – und schon sind Hacker mitten in der Produktion und können Produktionsstraßen oder Kraftwerke stilllegen oder sogar in Operationen eingreifen.

Um sich besser gegen Cyber-Risiken zu schützen, vertrauen immer mehr Unternehmen der Cloud und verlagern Teile ihrer Legacy-Anwendungen in die Clouds. Vor allem die Public-Cloud-Plattformen der großen Hyperscaler Amazon Web Services, Google Cloud und Microsoft Azure werden immer beliebter – auch für unternehmenskritische Anwendungen wie ERP, PLM oder CRM. Ein großer Vorteil der Cloud-Anbieter liegt in deren enormer Innovationsstärke – beispielsweise im Bereich der künstlichen Intelligenz zur Erkennung von Anomalien in den Netzwerken – und immer mehr Kunden halten das Sicherheitsniveau in der Public Cloud für am höchsten. Tatsächlich hat das Jahr 2020 den Durchbruch für die Cloud gebracht und die Zahl der Cloud-Migrationen steigt kontinuierlich an – diese Entwicklung wird sich fortsetzen.

Im Zusammenhang mit der zunehmenden Cloud-Transformation gewinnen Managed Cloud Service Provider weiter an Bedeutung, um die immer komplexeren hybriden IT- und Multi-Cloud-Landschaften zu betreuen. Diese Provider stellen, neben anderen Faktoren wie Security by Design und Security Operations Centers, in Zeiten des Fachkräftemangels einen wichtigen Baustein für eine erfolgreiche Cyber-Security-Strategie und damit für eine erfolgreiche, nachhaltige digitale Transformation dar.

Lünendonk im Gespräch mit Arvato Systems

CYBER SECURITY IST EINE FRAGE DES VERTRAUENS

Nach dem Angriff ist vor dem Angriff. Das wissen die Security-Experten von Arvato Systems aus ihrer langjährigen Erfahrung sehr genau. Im Interview mit Lünendonk schildern Arne Wöhler, Head of Business Consulting and Development Cyber Security, und Timo Schlüter, Business Consultant Cyber Security, wie Arvato Systems mit Managed Security Services für maßgeschneiderte Cyber Security in Unternehmen sorgt.

Arne Wöhler
Head of Business Consulting and Development Cyber Security bei Arvato Systems

„Die Bedrohungslage verändert sich permanent. Das zwingt uns als Dienstleister und IT Security Advisor, unsere eigenen Lösungen und Services ebenfalls kontinuierlich weiterzuentwickeln. Ansonsten wäre es uns nicht möglich, die Systeme unserer Kunden bestmöglich zu schützen."

Timo Schlüter
Business Consultant Cyber Security bei Arvato Systems

„Cyber Security ist nichts, das Unternehmen out-of-the-box beziehen könnten und auch keine Standard-Lösung. Cyber Security ist in unserer Definition ein Business-Prozess und muss in der gesamten Organisation verankert sein."

LÜNENDONK IM GESPRÄCH MIT ARVATO SYSTEMS

Cyber Security sollte strategisch gedacht werden

LÜNENDONK: Herr Schlüter, was verstehen Sie unter Cyber Security?

TIMO SCHLÜTER: Dem Begriff „Cyber Security" kann man sich zunächst sozusagen aus wissenschaftlicher Sicht nähern. In der Fachliteratur fasst man unter Informationssicherheit vier verschiedene Bereiche zusammen:

1. Computersicherheit, also den Schutz vor Systemausfällen, 2. Datensicherheit, also den Verlust und die Manipulation von Daten, 3. Datenschutz, also den Schutz sensibler Daten vor Missbrauch, und 4. IT-Sicherheit (Cyber Security), also den Schutz vor unerlaubtem Zugriff.

Um diesen Part der Informationssicherheit kümmern wir uns im Rahmen unserer Managed Security Services. Es geht primär darum, technische und soziotechnische Systeme – dazu zählen Menschen und Prozesse – zu schützen. Insbesondere der Mensch ist ein beliebtes Angriffsziel, man denke nur an Phishing-Mails oder Ähnliches.

LÜNENDONK: Wie kann man sich das nun in der Praxis vorstellen?

TIMO SCHLÜTER: In der Praxis greifen wir auf Prevention-, Detection- und Response-Maßnahmen zurück, gehen also weit über das klassische Kernangebot eines Security Operations Center (SOC) hinaus. Einfach ausgedrückt kann man sagen, Prevention dient dazu, Hacker von Systemen fernzuhalten, mit Detection lassen sich eingedrungene Hacker aufspüren und Response-Maßnahmen ermöglichen es, sie wieder aus den Systemen zu entfernen. Und in jeder dieser drei Säulen der Cyber Security berücksichtigen wir drei wesentliche Ebenen:

Da ist zunächst die Compliance, also alle Richtlinien und Vorgaben von Unternehmen, mit denen sie Cyber Security gewährleisten. Wichtig ist auch die technische Security. Darunter fallen zum Beispiel der Aufbau von Firewalls oder auch das Hardening von Systemen. Dazwischen befinden sich die Security Operations. Hier geht es um strategische Aspekte: Wie sind die Compliance-Vorgaben umzusetzen? Welche Prozesse braucht es dafür? Wie ist mit Daten umzugehen?

LÜNENDONK: Das klingt aber immer noch etwas theoretisch. Wie können Unternehmen denn in der Praxis ganz konkret erkennen, wie viel Cyber Security sie tatsächlich brauchen?

TIMO SCHLÜTER: Das kommt tatsächlich auf die individuelle Situation des Unternehmens an – hier gibt es keine pauschale Antwort. Cyber Security ist nichts, was Unternehmen „out-of-the-box" beziehen könnten. Cyber Security ist nie eine Standardlösung, sondern immer Ergebnis eines fortlaufenden Prozesses. Unternehmen

müssen sich darüber Klarheit verschaffen: Wie steht es um ihre Cyber Security? Welche Schwachstellen gibt es? Welche Systeme sind besonders schützenswert? Welches Security-Level ist sinnvoll? Das ist eine besonders wichtige Überlegung: Banken oder Chemieunternehmen müssen ein Höchstmaß an Sicherheit erfüllen, während für kleinere Händler ein niedrigeres Level vertretbar sein kann. Um genau solche Fragen zu klären, kommen wir dann häufig als Dienstleister ins Spiel.

LÜNENDONK: Wie kann im Rahmen einer solchen Zusammenarbeit ein sinnvolles Vorgehen rund um IT-Security aussehen?

TIMO SCHLÜTER: Zunächst ist es wichtig, in einem Workshop die bestehende IT-Infrastruktur zu analysieren. Wir schauen uns an, welche Systeme und gegebenenfalls auch Security-Produkte das Unternehmen einsetzt. Je nach Ergebnis dieser ersten Analyse sind verschiedene, unterschiedlich umfangreiche Maßnahmen zu ergreifen. Die gewonnenen Erkenntnisse übertragen wir in eine Security-Strategie samt Umsetzungs-Roadmap.

Wie die erarbeitete Lösung dann umgesetzt wird, ist eine höchst individuelle Angelegenheit, die vom vorhandenen Status quo in Sachen Cyber Security abhängt. Damit sich ein Projekt in einem finanziell vertretbaren Rahmen bewegt, klären wir gemeinsam mit dem Unternehmen: Welche Bereiche und Systeme sind besonders schützenswert? Wir sprechen hier gern von „Kronjuwelen". Und wie lässt sich das Beste aus dem Budget herausholen? Weil eine in wirklich jeder Situation 100-prozentige Sicherheit schlichtweg nicht möglich ist, geht es darum, die Balance zwischen vertretbarem Risiko und nötiger Investition zu finden.

LÜNENDONK: Was passiert in den eben erwähnten Security-Workshops?

ARNE WÖHLER: In den Workshops erarbeiten wir gemeinsam mit dem Unternehmen ein bedarfsgerechtes Konzept. Dabei gehen wir schrittweise vor. Beim Scoping legen wir fest, welche Kronjuwelen beziehungsweise Unternehmensbereiche im Fokus stehen sollen. Darauf folgt das Assessment. Hier beschäftigen wir uns detailliert mit dem Scope und führen eine Gap-Analyse durch. Dabei greifen wir auf die bewährte Vorgehensweise des Center for Internet Security, kurz CIS, zurück. Auf der Basis der mittels CIS-Scan aufgespürten Schwachstellen erarbeiten wir schließlich ein maßgeschneidertes Security-Konzept und clustern die erforderlichen Maßnahmen entsprechend ihrer Umsetzungspriorität.

Dabei ist das MITRE ATT&CK Framework unverzichtbar. Es listet alle bekannten Angriffstechniken auf und stellt wichtige Informationen zu ihrer Erkennung und zur Behebung damit verursachter Incidents bereit. Da neue Techniken im Wochenrhythmus auf den Markt drängen, wird das Framework fortlaufend aktualisiert. Wenn man ein Konzept erarbeitet, ist es wichtig zu wissen, dass Hacker zumeist auf eine bestimmte Branche spezialisiert sind. Solche spezifischen Informationen erhalten wir aus besonderen Datenbanken. Je nach Branche, in der das Unternehmen aktiv ist, erstellen wir dann eine Heatmap mit den wahrscheinlichsten Bedrohungen. Darauf legen wir dann unser Augenmerk: Wie ist ein Angriff erkennbar? Wie ist dagegen vorzugehen? Welche Maßnahmen sind sinnvoll?

LÜNENDONK: Wie kann ein entsprechendes Security-Konzept umgesetzt werden?

ARNE WÖHLER: Hier möchten wir betonen, dass ein Security-Konzept zunächst Empfehlungen gibt. Wie das jeweilige Unternehmen dann damit umgeht, ist individuell durch den Kunden zu entscheiden und hängt auch von dessen genauen Zielen ab. Kommt es für die Umsetzung des Konzepts dann zu einer fortgesetzten Zusammenarbeit, passen wir das bestehende MITRE ATT&CK Framework im Rahmen des Onboardings zunächst an die Prozesse des Kunden an und implementieren die erforderliche Technik.

In der Praxis wird es dann wirklich spannend. Mit dem Ziel, ein möglichst hohes Maß an Cyber Security sicherzustellen, unterziehen wir die Strategie und das Konzept ständig kritischen Checks und nehmen bei Bedarf Anpassungen vor. Denn die Bedrohungslage verändert sich permanent. Das zwingt uns als Dienstleister und IT Security Advisor, unsere eigenen Lösungen und Services ebenfalls kontinuierlich weiterzuentwickeln. Ansonsten wäre es uns nicht möglich, die Systeme unserer Kunden bestmöglich zu schützen.

LÜNENDONK: Wenn es dann tatsächlich doch zu einem Sicherheitsvorfall kommt – was sind dann die Voraussetzungen für eine erfolgreiche Abwehr?

ARNE WÖHLER: Für eine erfolgreiche Incident Response gibt es – wie bei jedem Krisenabwehrplan – mehrere Erfolgsfaktoren: Kommunikation, Organisation und Prozesse sowie Ressourcen. Daraus lassen sich einzelne Maßnahmenpakete präventiv ableiten und dokumentieren. Sie beschreiben das Ziel, die Vorgehensweise, die notwendigen Rollen samt involvierter Unternehmensbereiche und die nötigen Skills. Beispiele sind hier Domain Administration und Datacenter Management. Auch ein Incident-Response-Kommunikationsplan darf nicht fehlen.

Grundsätzlich lässt sich Incident Response in zwei Handlungsstränge aufteilen. Da wäre zunächst die forensische Untersuchung des vermeintlichen Vorfalls. Hier ist zu ermitteln, wie der Angreifer in die Infrastruktur eindringen konnte, welche Ziele er verfolgt, wie tief er eingedrungen ist und welche technischen Methoden er angewendet hat.

Um diese Fragen zu beantworten, ziehen Analysten Logging-Daten sowie Informationen der möglicherweise vorhandenen Endpoint Detection und des Netzwerk-Monitorings heran und analysieren auffällige Systeme bis in die Tiefe. Üblicherweise konzentriert sich die Untersuchung auf die Bereiche Active Directory, DMZ – das steht für „demilitarisierte Zone“, also eine Pufferzone als eigenständiges Netzwerk zwischen internem und externem Netzwerk – und die schon erwähnten Kronjuwelen, also besonders schützenswerte Bereiche.

Auf der Basis der Erkenntnisse geht es dann darum, Maßnahmen zur Abwehr des Angriffs und zur Entfernung des Angreifers aus dem Netzwerk zu planen. Bei laufenden Angriffen ist zu entscheiden, ob und welche Ad-hoc-Maßnahmen eingeleitet (Containment) und welche der vorbereiteten Maßnahmenpakete angewendet werden müssen.

Gleiches gilt für die Vorbereitung einer Remediation und deren Durchführung. Da sich Unternehmen im Hinblick auf Komplexität, Aufbau der Infrastruktur (Domains, Netzwerk, DMZ etc.), Monitoring-Fähigkeiten an Endpoints, Netzwerkverkehr und verfügbare Analyse-Skills unterscheiden, sind diese Maßnahmenpakete individuell anzupassen. Gleiches gilt für die notwendigen Abwehrmaßnahmen, die natürlich den Methoden und Techniken des Angreifers entsprechen müssen.

LÜNENDONK: Bei welchen konkreten Vorfällen muss ein Incident-Response-Plan schließlich greifen?

ARNE WÖHLER: Die Einschätzung, ob es sich um einen Sicherheitsfall handelt, nehmen typischerweise die Analysten des SOC vor. Sie bewerten das Gefahrenpotential und entscheiden gemeinsam mit dem Incident-Response-Team, ob ein potenzieller Verteidigungsfall vorliegt. Sollte es sich um einen massiven Sicherheitsvorfall handeln – von Erpressungsfällen mit Ransomware bis hin zu vermuteten APT-Angriffen –, übernimmt das Incident-Response-Team: Es koordiniert die notwendigen Eindämmungs- und Bereinigungsaktivitäten und führt sie durch.

LÜNENDONK: Viele Ihrer Kundenbeziehungen bestehen schon viele Jahre. Ist das im Security-Kontext ein Vorteil?

ARNE WÖHLER: Zumindest hilft es im Alltag. Insbesondere Cyber Security ist eine Frage des Vertrauens. Man stelle sich folgende Situation vor: Eines unter 500 Devices ist von Ransomware befallen. Es wäre ein Leichtes, das betroffene Gerät aus dem Netzwerk zu isolieren, um den Schaden einzudämmen.

Die Frage ist: Dürfen wir das – im Zweifel ohne Rücksprache –, um keine Zeit zu verlieren? Schließlich dringen wir in das Hoheitsgebiet des Unternehmens, in seine IT-Infrastruktur, ein. Ohne unbedingtes Vertrauen in seinen Dienstleister wird ein Unternehmen ein derartiges eigenständiges Vorgehen kaum befürworten.

Wir haben also den Anspruch, ein verlässlicher Partner für unsere Kunden zu sein. Sich regelmäßig offen auszutauschen ist eine wichtige, wenn nicht die wichtigste Voraussetzung für langfristig stabile und vor allem vertrauensvolle Kundenbeziehungen.

Ein relevanter Faktor ist auch Kosteneffizienz. Ein Dienstleister muss den vorgegebenen Budgetrahmen einhalten. Wenn das nicht gelingt, geht Vertrauen schnell verloren. Wir sind der Meinung: Nur in einer stabilen Partnerschaft können Cyber-Security-Konzepte nachhaltig erfolgreich sein.

Unternehmensprofile

ARVATO SYSTEMS

LÜNENDONK & HOSSENFELDER

UNTERNEHMENSPROFIL

Arvato Systems

Als international agierender IT-Spezialist und Experte für künstliche Intelligenz und Multi-Cloud-Services unterstützt Arvato Systems namhafte Unternehmen bei der digitalen Transformation. Rund 3.000 Mitarbeiter an weltweit über 25 Standorten stehen für hohes technisches Verständnis, Branchen-Know-how und einen klaren Fokus auf Kundenbedürfnissen. Als Team entwickeln wir innovative IT-Lösungen, bringen unsere Kunden in die Cloud, integrieren digitale Prozesse und übernehmen den Betrieb wie auch die Betreuung von IT-Systemen.

WIR BIETEN ...

- Umfassende IT-Lösungen für Branchen wie Handel, Medien, Gesundheitswesen sowie Energie- und Versorgungswirtschaft
- Langjährige Erfahrung in der digitalen Transformation
- Kompetenz in Themen wie künstliche Intelligenz, Cloud Computing, IT-Security, Customer Experience, E-Commerce und Business-Process-Management
- Know-how in vielen starken Technologien und ein ausgeprägtes Ökosystem mit Partnern wie Amazon Web Services, Google, Microsoft und SAP
- Eine große Bandbreite an Infrastructure-Services wie beispielsweise Managed Services sowie ein darauf aufbauendes Application Management

Zudem können wir im Verbund der zum Bertelsmann-Konzern gehörenden Arvato ganze Wertschöpfungsketten abbilden. Unsere Geschäftsbeziehungen gestalten wir persönlich und partnerschaftlich mit unseren Kunden. So erzielen wir gemeinsam nachhaltig Erfolge. Arvato Systems – Empowering Digital Leaders.

INFORMATIONEN RUND UM DAS IT-SECURITY-ANGEBOT VON ARVATO SYSTEMS:

E-Mail: CyberCare@arvato-systems.de
Internet: http://www.arvato-systems.de/security

KONTAKT

Arvato Systems
An der Autobahn 200
33333 Gütersloh
E-Mail: info@arvato-systems.de
Internet: http://www.arvato-systems.de

UNTERNEHMENSPROFIL

LÜNENDONK

Lünendonk & Hossenfelder GmbH

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Management- und IT-Beratung, Wirtschaftsprüfung, Steuer- und Rechtsberatung, Facility Management und Instandhaltung sowie Personaldienstleistung (Zeitarbeit, Staffing).

Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden Lünendonk®-Listen und -Studien heraus.

Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Unternehmer mit den Lünendonk-Service-Awards aus.

KONTAKT
Lünendonk & Hossenfelder GmbH
Mario Zillmann
Maximilianstraße 40, 87719 Mindelheim
Telefon: +49 (0) 8261 73140 – 0
Telefax: +49 (0) 8261 73140 – 66
E-Mail: zillmann@luenendonk.de
Internet: www.luenendonk.de

IMPRESSUM
Herausgeber:
Lünendonk & Hossenfelder GmbH
Maximilianstraße 40
87719 Mindelheim

Telefon: +49 (0) 8261 73140 – 0
E-Mail: info@luenendonk.de
Internet: www.luenendonk.de

Bilderquellen:
Titelseite: © Adobe Stock/ sasun Bughdaryan

Autor:
Mario Zillmann, Partner, Lünendonk & Hossenfelder GmbH

LÜNENDONK

ÜBER LÜNENDONK & HOSSENFELDER

Lünendonk & Hossenfelder mit Sitz in Mindelheim (Bayern) analysiert seit dem Jahr 1983 die europäischen Business-to-Business-Dienstleistungsmärkte (B2B). Im Fokus der Marktforscher stehen die Branchen Management- und IT-Beratung, Wirtschaftsprüfung, Steuer- und Rechtsberatung, Facility Management und Instandhaltung sowie Personaldienstleistung (Zeitarbeit, Staffing). Zum Portfolio zählen Studien, Publikationen, Benchmarks und Beratung über Trends, Pricing, Positionierung oder Vergabeverfahren. Der große Datenbestand ermöglicht es Lünendonk, Erkenntnisse für Handlungsempfehlungen abzuleiten. Seit Jahrzehnten gibt das Marktforschungs- und Beratungsunternehmen die als Marktbarometer geltenden Lünendonk®-Listen und -Studien heraus. Langjährige Erfahrung, fundiertes Know-how, ein exzellentes Netzwerk und nicht zuletzt Leidenschaft für Marktforschung und Menschen machen das Unternehmen und seine Consultants zu gefragten Experten für Dienstleister, deren Kunden sowie Journalisten. Jährlich zeichnet Lünendonk zusammen mit einer Medienjury verdiente Unternehmen und Unternehmer mit den Lünendonk®-Service-Awards aus.

- Wirtschaftsprüfung/ Steuerberatung
- Managementberatung
- Technologie-Beratung/ Engineering Services
- Informations- und Kommunikations-Technik
- Facility Management/ Industrieservice
- Zeitarbeit/ Personaldienstleistungen

Erfahren Sie mehr unter
http://www.luenendonk.de

MARKTFORSCHUNG UND MARKTBERATUNG AUS EINER HAND