ASSECOR splone

Resiliente IT-Infrastrukturen

Wie Sie Ihre Organisation für die Zukunft rüsten

Ausgabe 2023

1. IT-Sicherheit und KMUs: Es ist kompliziert

Wer sich bemüht – und die entsprechend notwendige kriminelle Energie aufbringt -, der findet auf einschlägigen Webseiten das nötige Wissen, um Schwachstellen bei Unternehmen relativ unkompliziert ausnutzen zu können. Dabei muss man nicht einmal IT-Fachkenntnisse mitbringen, häufig reichen schon einfache Tricks, um Menschen Geheimnisse zu entlocken. Dabei ist noch gar nicht die Rede von spezialisierten IT-Attacken.

2021/22 gab es jeden Tag bis zu 400.000 neue Varianten von Schadsoftware, so das BDI in ihrem jüngsten Bericht zur „Lage der IT-Sicherheit in Deutschland". Zu den Top 3 der Bedrohungen für die Wirtschaft zählen laut BDI neben Ransomware auch falsch konfigurierte Online-Server oder eine korrumpierte IT-Supply-Chain. Weil die Attacken immer professioneller werden, ist es umso wichtiger, sich eingehend zu schützen.

Fragile Altsysteme

Alles schön und gut. Aber ähnlich, wie Gebäude oder Straßen an Verschleiß leiden und erneuert werden müssen, bedarf auch die IT-Infrastruktur von Zeit zu Zeit Auffrischungen hinsichtlich Funktionalität und Sicherheit. Der technologische Wandel bei IT-Systemen verläuft mittlerweile allerdings derart schnell, dass insbesondere kleine und mittelständische Unternehmen (KMUs) nicht mehr hinterherkommen. Unternehmen können oft nicht alle Aspekte der IT-Sicherheit abdecken: sei es wegen der geringen Flexibilität und mangelnder Skalierbarkeit laufender Software, aufgrund einer hohen Instabilität, oder wegen fehlender Abwehrmechanismen von Schadsoftware. Die verwendete Technologie ist dabei lediglich eine Seite der Medaille. Ein wichtiger Aspekt der generellen IT-Resilienz hat mit der menschlich-sozialen Komponente zu tun: die konsequente Schulung des Personals ist unabdingbar! Eine widerstandsfähige Infrastruktur, bei der alle Facetten berücksichtigt werden, bedarf der akribischen Planung.

Dass bei vielen Unternehmen massiver Aufholbedarf besteht, zeigt auch eine Umfrage des IDC aus dem Jahre 2019 500 befragten Unternehmen aus über 10 Branchen[1]:

- Nur 11,4 % der Befragten verfügen über eine sehr ausgereifte IT-Resilienz
- 90% der Befragten wollen ihre Investitionen in die IT-Resilienz in den nächsten zwei Jahren erhöhen

Dieser Trend setzt sich bis in die Gegenwart fort: so mahnt etwa der Cyber Resilience Act der EU aus dem Jahre 2022 die Gefahren der extensiven Vernetzung an: „when everything is connected, a cybersecurity incident can affect an entire system, disrupting economic and social activities."

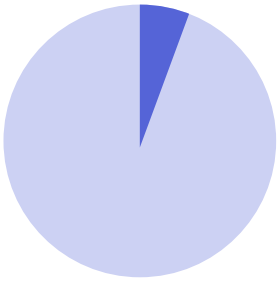
Cyberkriminalität nimmt weiter zu

Man darf dabei nicht vergessen, dass das auch kritische Unternehmensdaten betrifft. Wirft man einen Blick in die Presse, stellt man schnell fest, dass viele Unternehmen hier unvorbereitet sind und weit weg davon, schnell die richtigen Maßnahmen ergreifen zu können. Verzweifelte Unternehmen schaffen es nicht, ihre IT-Systeme vor Einbrüchen zu sichern und zahlen zunehmend höhere Lösegelder an Hacker-Organisationen. Durch solche Attacken wird nicht selten der gesamte Betriebsablauf unterbrochen, da Hacker immer besser vorbereitet sind und im Vorhinein ganz ausführlich studieren, welche kritischen Daten eines Unternehmens ein lohnendes Ziel darstellen und wo die jeweiligen Schwachstellen liegen.

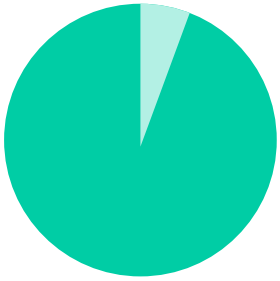
IT-Resilienz hat viele Gesichter: es existiert eine Vielzahl an Einfalltoren für Cyberkrimininelle, die es zu sichern gilt. Die Hacker-Szene entwickelt sich weiter und reagiert kurzfristig auf aktuelle Ereignisse. Zum Beispiel entstanden während der Corona-Pandemie plötzliche hohe Nachfrageschwankungen und Engpässe in überlasteten IT-Systemen, die zu einer Server Downtime führen konnten. An dieser Stelle fehlte es an flexiblen Skalierungsmöglichkeiten, eine Schwachstelle und auch ein Aspekt der IT-Resilienz.

Dabei sollten gerade KMUs für ihre weitere Wettbewerbsfähigkeit anpassungsfähiger als große Unternehmen sein, leben sie doch in der Regel von flacheren Hierarchien, kürzeren Entscheidungswegen und weniger bürokratischen (agilen) Strukturen.

Im folgenden Whitepaper werden wir behandeln, was eine IT-resiliente Infrastruktur ausmacht und wie KMUs hier vorgehen sollten, um besser für die Zukunft gerüstet zu sein.



11, 4 %
der Befragten verfügen über eine sehr ausgereifte IT-Resilienz



90 %
der Befragten wollen ihre Investitionen in die IT-Resilienz in den nächsten zwei Jahren erhöhen

1 *IDC: The State of IT Resilience, Whitepaper, 2019*

2. Was ist eine resiliente IT-Infrastruktur? Und was gehört alles dazu?

Die Definition des branchenweisen Bitkoms bezeichnet „IT-Resilienz“ als die „Fähigkeit, eine innere Widerstandsfähigkeit gegenüber Krisen und Belastungen zu zeigen.“[2] Das klingt erstmal einfacher als es ist. Diese „innere Widerstandsfähigkeit“ zieht sich durch die gesamte IT-Infrastruktur sowie IT-Organisation und sollte durchgängig als strategische Komponente miteinbezogen werden. Einige Trendthemen in diesem Bereich seien hier exemplarisch erwähnt: zum Beispiel die für das Home-Office oder standortunabhängiges Arbeiten unablässige IT-Infrastruktur, oder eben die verlässliche und dabei sichere Skalierbarkeit der verwendeten IT-Systeme. Es gibt aber auch klassischere Themen, die Hand in Hand gehen mit diesen Trends: die Aufteilung der IT-Systeme in cloud oder on premise ist ein solches. Die eingehende Schulung von Mitarbeitenden, die potentielle Schwachstellen, oder aber die IT-Sicherheit selbst sein können, ist ein anderes. IT-Resilienz, soviel ist sicher, funktioniert nur im Gesamtverbund aller beteiligten Aspekte:

Eine IT-resiliente, also eine widerstandsfähige Infrastruktur, die an alle Facetten denkt, sollte von Anfang an gut durchdacht und laufend aktuell gehalten werden.

IT-Resilienz bezieht sich auf die generelle Fähigkeit einer Organisation oder eines Unternehmens, IT-Systeme und entsprechende Prozesse so zu gestalten, dass sie widerstandsfähig gegenüber situativen Störungen und (kriminellen) Bedrohungen sind. Das erklärte Ziel der Etablierung resilienter IT-Strukturen ist es, sowohl den Fortbestand der Geschäftstätigkeit sicherzustellen als auch die Sicherheit verwendeter Daten und Programme zu garantieren.

Die Maßnahmen, die die IT-Resilienz einer Organisation zu verbessern versprechen, gliedern sich in zwei grobe Richtungen auf: einerseits referieren sie auf ein Finetuning der Prozesse, andererseits umfassen sie die Implementierung neuer Soft- bzw. Hardware. So steht die regelmäßige Überprüfung und ggf. die Aktualisierung von IT-Sicherheitsmaßnahmen weit oben auf der Liste der Prozessanpassungen, das Aufsetzen starker Firewalls und die Einführung von Verschlüsselungstechnologien für Datenübertragung und die respektive Speicherung dieser Informationen impliziert neben der sorgfältigen Schulung des Personals auch die adäquate Verwendung moderner Soft- und Hardware. IT-Resilienz bedarf somit eines über weite Strecken komplementären Ansatzes, der sowohl soziale wie auch materielle Aspekte umfasst.

Nur mit entsprechenden ganzheitlichen Maßnahmen und einer transparenten Strategie zur IT-Resilienz lässt sich eine funktionierende IT-Infrastruktur umsetzen.

Beim vom ifaa erarbeiteten „Resilienzkompass“ kommt die Verschränkung von Techno- und Soziosphäre stärker zur Geltung: er bezieht neben der verwendeten „Strategie“ und den „Prozessen“ auch Aspekte wie „Führung“ oder „Mitarbeitende“ explizit mit ein.[3] Nur, wenn die IT-Infrastruktur ganzheitlich gedacht wird und mit der Arbeitsweise der Mitarbeitenden harmoniert, lässt sich eine kohärente Strategie zur IT-Resilienz umsetzen.

Abschließend lässt sich an dieser Stelle festhalten, dass die Umsetzung von Maßnahmen, die die IT-Resilienz begünstigen, zwar eine Mammutaufgabe ist; sie macht sich aber langfristig mehr als bezahlt! Sind die Prozesse einmal optimiert, lässt sich auf ihrer Grundlage weitgehend frei arbeiten. Es hat etwas Befreiendes, im Angesicht der Krisen unserer Zeit, nicht länger um die Funktionstüchtigkeit der Infrastruktur bangen zu müssen, sondern sich mit Hand und Herz seinem Kerngeschäft widmen zu können. IT-Resilienz ist dementsprechend eines der Themen unserer Zeit.

2 Bitkom: „Resilienz – Stärkung für zukünftige Herausforderungen“, Online-Beitrag von Ralf Kreutzer, 2021 https://bitkom-akademie.de/news/resilienz-staerkt-fuer-kuenftige-herausforderungen
3 ifaa – Institut für angewandte Arbeitswissenschaft: Resilienzkompass zur Stärkung der individuellen und organisationalen Resilienz in Unternehmen, 2018, S. 11.

Das Gerüst der IT-Resilienz

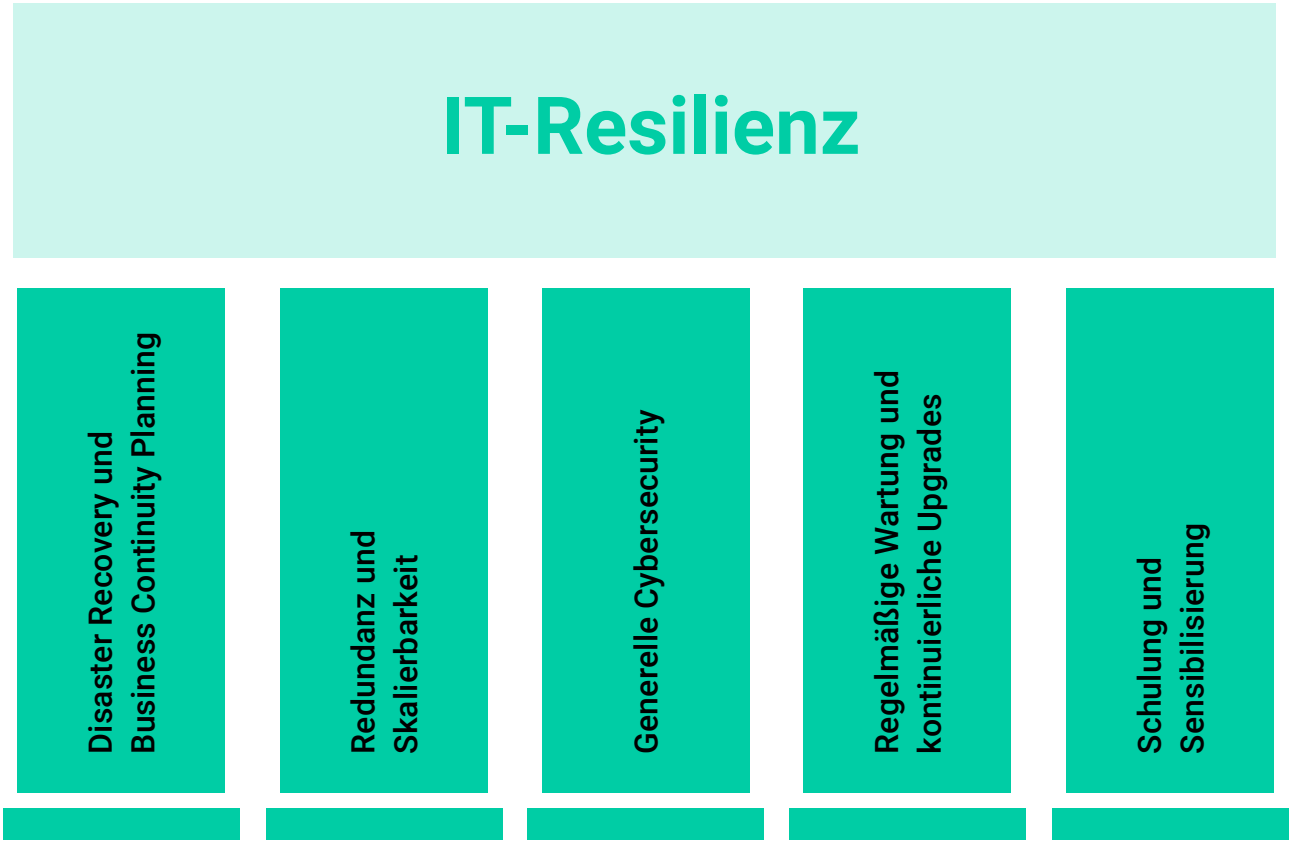


Abbildung: eigene Darstellung

Disaster Recovery und Business Continuity Planning
Die Entwicklung von Plänen zur Wiederherstellung nach einem Ausfall und zur Aufrechterhaltung des Geschäftsbetriebs kann dazu beitragen, die Auswirkung von Ausfällen zu minimieren und sicherzustellen, dass ein Normalbetrieb der jeweils betroffenen Systeme schnell wieder sichergestellt werden kann.

Redundanz und Skalierbarkeit
Die Implementierung von redundanter Infrastruktur und die Fähigkeit, IT-Systeme bei Bedarf skalieren zu können, kann die Resilienz erhöhen und sicherstellen, dass Ihr Unternehmen auch weiterhin in der Lage ist, seine Geschäftsfähigkeit aufrechtzuerhalten. Eines der einfachsten Mittel, um eine redundante und skalierbare Funktionalität zu gewährleisten, ist die Verlagerung essenzieller Prozesse in die Cloud. Die emphatisch dezentrale Eigenlogik der Cloud stellt sicher, dass Datenflüsse weitestgehend stabil bleiben, selbst, wenn einmal ein Teilsystem ausfallen sollte. Zudem zeichnen sich Cloudlösungen durch die Möglichkeit aus, weitgehend unabhängig von der Hardware erweitert werden zu können.

Generelle Cybersecurity
Die Schaffung robuster Sicherheitsmaßnahmen, einschließlich der Integration von Firewalls, Encryption und Authentifizierungsmechanismen, kann dazu beitragen, Cyberangriffe direkt abzuwehren oder aber zumindest wesentlich abzuschwächen und so die Integrität der IT-Systeme zu schützen.

Regelmäßige Wartung und kontinuierliche Upgrades
Die Etablierung bestimmter Wartungs- und Upgrade-Routinen erlauben es, etwaige Probleme bereits im Voraus zu erkennen und sie fachgerecht zu beheben, bevor diese zu potenziellen Ausfällen führen.

Schulung und Sensibilisierung
Zusätzlich zu den bisher genannten Maßnahmen ist auch ein Bewusstsein der Mitarbeitenden zu forcieren, das individuell für den Ernstfall zu wappnen vermag. Nur, wenn die Beschäftigten eingehend informiert sind und wissen, wie sie sich in einer sicherheitsrelevanten Notlage zu verhalten haben, zeitigen die getroffenen Maßnahmen auch adäquate Effekte.

3. Use Cases

In den nachfolgenden exemplarischen Use Cases werden gleich mehrere für die IT-Resilienz relevante Bereiche behandelt und von der Ausgangssituation bis zur Lösung konstruiert. Die Unternehmen kommen aus dem Transport- bzw. Energiesektor. Eins der beiden Unternehmen ist im Bereich der kritischen Infrastrukturen (kurz: „KRITIS“) angesiedelt. Im Hinterkopf sollte man daher behalten, dass Betreiber kritischer Infrastrukturen in der Regel gut gegen Cyberangriffe und IT-Ausfälle gerüstet sind, aber dafür auch kontinuierlich in ihre IT-Sicherheit investieren müssen.

Im folgenden sollen relevante Aspekte der IT-Resilienz anhand zweier Use Cases näher erläutert werden.

Eine der größten Herausforderung liegt damit im organisch gewachsenen IT-Monolithen selbst: Die Prozesse des Systems sind derart verwoben, dass es schwierig ist, sie zu sezieren. Das ist aber notwendig, um einzelne Funktionen abzutrennen und gegebenenfalls mit moderneren technologischen Mitteln umzusetzen.

Hinzu kommt, dass bei einem Altsystem oft nicht alles dokumentiert ist oder bereits existierende Dokumentationen veraltet sind. Etwaige Folgen einer „Sezierung“ bezüglich der Funktionalität sind somit nicht vorhersehbar.
Bei dem Aufsetzen einer neuen Software gilt es von Anfang an akribisch zu dokumentieren und so einen rebungslosen Wissenstransfer in der Zukunft zu ermöglichen.

Use Case 1

KRITIS: Einsatzplanungstool für Transportunternehmen

Der betreffende Kunde stand vor einer schwierigen Aufgabe: Die Aktualisierung eines Altsystems stand ins Haus. Dabei galt es allerdings, den Betrieb keinesfalls zu stören, um Ausfälle der Infrastruktur nach Möglichkeit zu vermeiden. Ob dieser Ausgangslage war schnell klar, dass eine Big-Bang-Umstellung auf ein komplett neues System mit großen Risiken verbunden gewesen wäre. Daher entschied sich das Transportunternehmen dazu, den IT-Monolithen bzw. das Altsystem nach und nach zu erneuern.

Ein solch modulares Vorgehen erlaubt ein sukzessives Herausschneiden von Funktionen, ohne den Gesamtverbund zu gefährden. Damit können Verbesserung und Portierung auf neue Technologiestandards gewährleistet werden, während das Altsystem gleichzeitig weiterhin zuverlässig seinen Dienst verrichtet. Gerade für KRITIS-Betreiber ist dieser stabilisierende Umstand besonders wichtig.

Ein solch grundlegender Umbau der digitalen Architektur bot dem Verkehrsunternehmen die Chance, eine ganzheitlich zukunftsorientierte IT-Strategie auszuarbeiten.

Ausgangslage

Bislang wird die Software des Kritis-Betreibers hauptsächlich für die Personaleinsatzplanung der Fahrzeugführer sowie die Anbindung direkt angrenzender Fremdsysteme genutzt. Dabei bildet das seit 20 Jahren laufende System alle für den Betrieb notwendigen Domänen ab (z.B. Personal- und Arbeitszeitverwaltung, Fahr- und Auftragsplanung sowie -bearbeitung, Arbeitszeiterfassung- und nachweise, etc.).

Alle Herausforderungen auf einen Blick

- Eine **veraltete Technologie** und organisch gewachsene IT-Architektur, die zu wuchern beginnt. Die Codebasis und damit die Prozesse sind technisch derart miteinander verwoben, dass es nahezu unmöglich ist, einzelne Funktionalitäten abzutrennen.
- Ein situativer Zuwachs an Systemkomplexität führt zu einem **Verschlankungsbedarf**.
- Es ist **kein (sofortiger) Komplettumstieg möglich** (kein „Big-Bang“-Umstieg).
- Der „veraltete“ Monolith muss weiterhin gewartet werden und **stets verfügbar sein**.
- Stete Weiterentwicklung und Anpassungen von Funktionen sind notwendig um **gesetzlichen und betrieblichen Anforderungen gerecht zu werden.**
- **Inhouse sind keine personelle Ressourcen** für Softwareentwicklung und Wartung vorhanden.
- Zusätzlich sind ein guter IT-Support und solides Testing nötig.

Das definierte Ziel

Das oberste Ziel für KRITIS-Betreiber ist immer die garantierte Aufrechterhaltung der Systemverfügbarkeit. Zu den Kernaufgabe zählt also, das Fortwirken des Systems sicherzustellen, eklatante Schwachstellen auszumerzen und darüber hinaus Prozesse und respektive Funktionalitäten zu verschlanken.
Langfristig soll das System auf einer modernen IT-Architektur fußen. Alle Ziele können nur im Verbund zu einer erhöhten Resilienz beitragen und das System langfristig effektiv, effizient und krisensicher machen.

Die Umsetzung

- **Aufbau einer kohärenten Wissensdatenbank** samt vollständiger Dokumentation der vorhandenen Legacy-Systeme und Altbestandteile
- **Erstellung eines IT-Bebauungsplans** für Teile der Architektur sowie Dokumentation der Datenflüsse
- Anwendung des strategischen **Domain Driven Designs**
- Beratung und Sensibilisierung des Kunden hinsichtlich der Risiken für die IT-Sicherheit
- **Gemeinsame Erarbeitung einer kohärenten IT-Strategie**
- **Etablierung zukunftsfähiger Prozesse**
- Weiterführung der **Wartung des Altsystems**
- **„Weiterentwicklung"** des Monolithen mit Augenmaß, d.h. zunächst so wenig wie irgend möglich im bestehenden System erweitern / ändern.

Spotlights für einen detailierten Überblick

Domain driven Design
Um in einem sehr komplexen System Struktur zu schaffen, wurde sich für eine Lösung der Softwareentwicklung entlang des strategischen Domain Driven Design (kurz: „DDD") entschieden. Das ist im Grunde sehr simpel: Domänen werden definiert und Kernprozesse herausgearbeitet. Das Gute dabei ist: mit aufgebautem Domainwissen werden Entwickler:innen dazu befähigt, die Fachprozesse zu verstehen und eine einheitliche Projektsprache zu sprechen - sowohl was die Softwareentwicklung anbelangt als auch die Dokumentation betreffend. Das gewährleistet einen nachhaltigen Wissenstransfer.
Der Ansatz des DDD ist dementsprechen ein solcher, der aus der menschlichen Praxis heraus entwickelt wird, weniger ein solcher, der strikt auf die technischen Voraussetzungen und Limitationen referiert. Es soll vermieden werden, dass sich Nutzer:innen den technischen Gegebenheiten eines Systems anpassen müssen, viel eher sollen sich systemische Prozesse den Nutzer:innen anpassen.
Da IT kein Selbstzweck ist, sondern vielmehr ein Mittel zur Erreichung anderer Ziele, sollen Entwickler:innen befähigt werden, einen jeweiligen Prozess innerhalb eines komplexen Systems bestmöglich technisch abzubilden. DDD liefert dabei ein Framework, das dabei hilft, rein technische und praktische Aspekte zu identifizieren, sie zu entflechten und ggf. zu ersetzen.

Steigerung der IT-Resilienz durch Wissenstransfer
Durch das sukzessive Herausschneiden einzelner Funktionen kann ein zerfasertes IT-System auf den modernsten technologischen Stand gebracht werden - gleichzeitig wird der bestehende Monolith solange entsprechend gewartet, bis die Umstellung auf eine modulare Lösung abgeschlossen ist. Die sach- und fachgerechte systeminterne Komplexitätsreduktion kann dabei als wichtiger Faktor die IT-Resilienz betreffend gelten. Unnötige Fuktionen und überflüssige Code-Residuen können die nachgelagerte Wartbarkeit langfristig ungemein erschweren. Zudem wird es durch die strukturelle Vereinfachung sowohl wesentlich einfacher, neue Mitarbeitende sorgfältig einzuarbeiten und sie adäquat an das System heranzuführen als auch eine nachhaltige Dokumentation zwecks zukunftssicheren Wissenstransfers zu garantieren.

IT-Strategie & entsprechende Methoden
Der Kunde wurde sowohl bei der Formulierung der generellen IT-Strategie als auch hinsichtlich der spezifischen Projektmanagement-Methode unterstützt.
Bei der Projektmanagement-Methode wählte der Kritis-Betreiber in gemeinsamer Absprache eine agile Vorgehensweise bezüglich der Weiterentwicklung: in Anlehnung an das Framework Scrum wurden Kanban-Boards mit Priorisierung für Wartungsarbeiten eingeführt. So war es möglich, dem Kunden den besten Service zuteil werden zu lassen.
Gerade ein Projekt mit einem hohen Komplexitätsgrad und zahlreichen Stakeholdern, die Koordination und Planung optimieren und für die ein regelmäßiger Austausch somit essenziell ist, profitiert ungemein von dieser Methodologie.

Use Case 2

Der resiliente, digitale Arbeitsplatz mit Office 365

Die Corona Pandemie lieferte für viele Unternehmen die Initialzündung bezüglich der generellen Auseinandersetzung mit einer weitreichenden Digitalisierung essenzieller Geschäftsprozesse und der zugehörigen Elaboration von Remote Work. Der Arbeitsalltag aus dem Homeoffice war unterdessen für einen Großteil der Mitarbeitenden völlig neu, ungewohnt und herausfordernd. Neben der sozialen Komponente, existierten auch solche Schwierigkeiten, die vorwiegend technischer Natur waren und eng mit den Limitationen der respektiven Infrastruktur zusammenhingen.

Ausgangslage

Die Möglichkeit der exzessiven Telepräsenz bedarf belastungsfähiger Software, adäquater Ausstattung der Räumlichkeiten als auch eines geschulten Umgangs mit Kamera, Mikrofon und VPN. Kurz gesagt: mobile Arbeit und deren adäquate Umsetzung avancierte innerhalb kürzester Zeit zu dem bestimmenden Thema innerhalb vieler Organisationen und Unternehmen.

Mitarbeitende mussten sich umgewöhnen und neue Routinen etablieren, die weiterhin effizientes Arbeiten garantierten; auf Erfahrungswissen konnten sich nur die wenigsten stützen. Die IT-Services waren neu, die Nutzer-Oberflächen teilweise anders und bekannte Funktionen wie das Drucken oder das interne Verteilen von Dokumenten gestalteten sich entweder schwer, oder waren so nicht vorhanden. Der verschlüsselte Mail-Transfer, oder die Encryption in der Cloud standen nun an der Tagesordnung. Dies sind nur einige wenige Beispiele, die im Arbeitsalltag im Homeoffice aufzutreten pflegten.

Alle Herausforderungen auf einen Blick

- Die engagierte **Einführung von belastungsfähigen Routinen für das Home Office**
- **Schaffung von Sicherheit** sowohl auf Soft- wie auf Hardwareebene
- Ausarbeitung von entsprechenden **Verhaltensregeln** für Mitarbeitende außerhalb der Büroräume
- **Resonanz zwischen Hard- und Software** um Effizienz auch Remote zu garantieren

Das definierte Ziel

Das Wichtigste hinsichtlich der Ermöglichung zeitgemäßer Arbeitsweisen, ist die Sicherstellung der kontiuierlichen Funktionsfähigkeit des Betriebs als Ganzes. Es geht also vor allem darum, die gelebte Praxis und die genutzten Tools miteinander in EInklang zu bringen und Sicherheit im Umgang mit den wesentlichen Materialien zu vermitteln.

Bezüglich der Implementierung von umfassenden Remote-Work-Lösungen existieren grob gesagt zwei Typen von Unternehmen:

1. Unternehmen, die sich proaktiv an der konstanten Weiterentwicklung der Arbeitswelt beteiligen
2. Unternehmen, die sich eher reaktiv verhalten

Bei besagtem Unternehmen handelt es sich um einen langfristigen Bestandskunden; es war dementsprechend eines jener Unternehmen, der ersten Gattung, die proaktive Vorkehrungen getroffen hatten. Es wurde ein grundlegendes Update der IT-Infrastruktur eingeleitet, bei dem sukzessive alle technischen Komponenten auf den Prüfstand gestellt wurden und für ein großes Update folgen sollte. Alltägliche Prozessroutinen auf Seiten der Mitarbeitenden wurden analysiert und belastungsfähige Strategien entwickelt, die diese krisensicher einzubinden erlaubten. Ein wichtiger Aspekt war die IT-Sicherheit.

Aspekte der Strategie waren:

- Beschaffung der entsprechenden Hardware
- Organisatorische Maßnahmen wie Richtlinien zu mobilen Arbeiten, Umgang mit Passwörtern, Tools für Video-Konferenzen oder die sachgerechte Verschlüsselung der Festplatte
- Technische Maßnahmen (VPN, MFA, Load Balancer)
- IT-Sicherheit: Regelungen zur Klassifizierung von Informationen und Daten sowie zum Datenmanagement

Fragen zur IT-Sicherheit waren vor allem: Was ist notwendig um auch weiterhin vertrauliche Daten wie z.B. Personalakten, Verträge oder Abrechnungen bearbeiten zu können, ohne den Verlust der Vertraulichkeit, der Verfügbarkeit oder der Integrität zu riskieren? Und wie können die Mitarbeitenden erfolgreich in diese Entwicklung eingebunden werden?

Gemeinsam mit Vertretern der einschlägigen Fachbereiche wurde untersucht, wie die bereits bestehenden Prozesse in den Arbeitsalltag integriert wurden und wie diese zukünftig an einem anderen Standort - unterwegs oder im Homeoffice - zum Tragen kommen können, ohne auf die notwendige IT-Sicherheit oder grundlegende Resilienz zu verzichten.

Die Umsetzung

- Ermittlung von **Schulungsbedarf** und Durchführung konsekutiver **Workshops**
- Beschaffung der entsprechenden **Hardware**
- Organisatorische **Maßnahmen** wie Richtlinien zu mobilen Arbeiten, Umgang mit Passwörtern, Tools für Video-Konferenzen oder die sachgerechte Verschlüsselung der Festplatte
- **Technische Maßnahmen** (VPN, MFA, Load Balancer)
- IT-Sicherheit: **Regelungen** zur Klassifizierung von Informationen und Daten sowie zum Datenmanagement

Schnell war klar, dass es sich vor allem beim Change Management und beim adäquaten Wissenstransfer um wichtige Komponenten handelt, um die IT-Sicherheit zu fördern. Alle noch so sinnvollen Tools helfen nichts, wenn Mitarbeitende nicht mit ihnen umzugehen vermögen.

Schulungsbedarf ermitteln

Die gewonnenen Daten wurden genutzt, um den individuellen Schulungsbedarf zu identifizieren. Das entwickelte Schulungskonzept fördert nicht nur die kurzfristige Umstellung, sondern fungiert durch seine iterative Natur auch langfristig unterstützend. Es geht mehr um betriebene Praxis, denn um eine einmalige Einführung. Unregelmäßig zu tätigende Updates, sich ändernde Interfaces oder neu eingeführte Funktionen können bei vielen Mitarbeitenden zu Frustrationen führen; dem gilt es aktiv entgegenzuwirken.

Schulungsreihen anbieten

Das finale Konzept sah eine kohärente Schulungsreihe zu Beginn vor, die sich durch einführende Online-Seminare unterstützt sah. Die aufbereiteten Aufzeichnungen dieser Veranstaltungen ermöglichte es den Mitarbeitenden auch zu einem späteren Zeitpunkt auf die Inhalte zugreifen zu können. Für die zukünftige Arbeit mit den neuen IT-Services erstellte das Rollout-Team eine gemeinsame digitale Agora, auf der aktuelle Infos zu neuen Updates zu finden sind. Darüber hinaus können an dieser zentalen Stelle allgemein wiederkehrende oder auch aktuell spezifische Fragen an IT-Service-Manager gestellt und beantwortet werden. Ein weiterer Bereich liefert den Nutzer:innen hilfreiche Tipps und Tricks, die sie im Alltag nutzen können. Andere Medien, wie z.B. ein interner Podcast, rundeten die Maßnahmen ab.

Warum Datenschutz und Informationssicherheit so wichtig werden

Routinen die zuvor Orientierung boten, existieren im Homeoffice häufig nicht mehr auf dieselbe Weise; die Grenzen zwischen Arbeits- und Freizeit verschwimmen unterdessen zusehends, worunter nicht zuletzt die Vorsicht leidet. Jedes Unternehmen verfügt über sensible Daten, die nur von all jenen verarbeitet werden dürfen, die für die Verarbeitung zwingend erforderlich sind (Need-to-Know-Prinzip). Hierzu zählen etwa Personaldaten wie Vertragsanpassungen, Gehaltsinformationen oder auch archivierte Krankschreibungen. Konsequente Sicherheit hängt dementsprechend von der Einhaltung klarer Regeln ab; auch und gerade in einer Welt, die sich immer stärker vom physischen Büro emanzipiert ist die Referenz auf klar umrissene Protokolle unabdingbar.

Use Case 3

Pentesting im Rahmen der KRITIS

Mit der zunehmenden Digitalisierung steigen auch die Risiken. Gerade Betreiber kritischer Infrastrukturen und systemrelevante Unternehmen sehen sich nicht allein mit strenger werdenden gesetzlichen Anforderungen konfrontiert, sondern auch mit konkreten technischen Herausforderungen. Ein möglicher Schaden hat auch gesellschaftliche Relevanz, weil er nicht auf das verantwortende Unternehmen begrenzt ist.

Ausgangslage

Im Lichte des wachsenden IT-Sicherheits- und -Resilienz-Bewusstseins kam der Kunde initial auf uns zu. In gemeinsamen Vorgesprächen wurden sowohl die Ausgangslage wie auch die respektiven Ziele identifiziert. Die Umsetzung der IT-Sicherheit wurde bisher von der internen IT-Abteilung verantwortet. Eine differenzierte Erfassung möglicher Risiken gab es entsprechend nicht. Das Identifizieren von Schwachstellen war bisher aus Mangel an Kapazitäten beim Kunden nicht abzubilden. Als Konsequenz wurden in Resonanz mit dem Kunden zwei explizite Ziele formuliert.

Ziel

Ein Penetrationstest ist nur eine von vielen Maßnahmen, um IT-Sicherheit zu begreifen und zu verbessern. Damit ein solcher Test aussagekräftig wird, gilt es, sich auf präzise Ziele zu konzentrieren. Gemeinsam mit dem Kunden wurde herausgearbeitet, dass es wichtig sei, mögliche Schwachstellen in einer Außensicht auf das Unternehmen genauso wie aus der Innensicht erfahrbar zu machen. Für KRITIS-Unternehmen ist es besonders wichtig, nicht allein auf die traditionelle IT zu schauen, sondern auch die Dimensionen der OT (Operation Technology), Leitstellen und/oder Industriesysteme zu berücksichtigen. Auch externe Systeme wie Trafos oder Pumphäuser sollten

im Rahmen eines entsprechenden Tests berücksichtigt werden. Neben den zu untersuchenden Systemen (engl. scope) wurde sich außerdem auf einen konkreten Zeitplan verständigt, der klare Deadlines für die finalen Ergebnisse beinhaltete.

Penetrationstest

Um die herausgearbeiteten Ziele zu erreichen, war es wichtig, die jeweils passenden Kolleg:innen in den Test einzubeziehen. Nur in den selstensten Fällen verfügen einzelne Personen über alle nötigen Kompetenzen. Es galt demenstsprechend Expert:innen für Social Engineering, Exploitation, Industrie-Sicherheit oder Windows-Netzwerke an einen Tisch zu bringen und sich vorbereitend abzustimmen. Einige Aspekte des Tests wurden ohne Vorabinformationen als Blackbox-Test durchgeführt, bei anderen war eine enge Zusammenarbeit mit dem Kunden zielführend und effizient. Im Rahmen des Tests konnten die verschiedenen Angriffsvektoren identifiziert und eingehend evaluiert werden. Eine akribische Dokumentation erlaubt ein hohes Maß an Nachvollziehbarkeit der Schwachstellen, sortiert die Schwachstellen nach branchenüblichen CVSS-Standards ein und liefert kohärente Lösungsvorschläge, die im Ergebnis helfen sollen, den Schwachstellen in behebender Manier zu begegnen.

Ergebnis

Nach erfolgreichem Ablauf des Tests wurden die Ergebnisse mit dem Kunden gemeinsam besprochen. Auf entscheidende Erkenntnisse wird hierbei stets besonders eingegangen. Im Ergebnis wurden dem Kunden nicht nur vorher unbekannte Schwachstellen sichtbar gemacht, es wurden ebenfalls konequente Reformen eingeleitet. So wurde als Folge des Tests das unternehmenseigene physikalisches Zugangssystem grundlegend überarbeit und potenziell anfällige Digitalsysteme zusätzlich abgesichert. Die sichtbar gewordenen Risiken zogen überdies eine Erweiterung der Qualitätsanforderungen an Zulieferer um notwendige IT-Sicherheitsaspekte nach sich. Zusätzlich wurden weitere Kapazitäten für die Sicherstellung der IT- und OT-Sicherheit geschaffen.

Alle Herausforderungen auf einen Blick

- **Systemimmanente Schwachstellen** waren weitgehend unbekannt
- Eine differenzierte **Evaluation möglicher Risiken** fand bisher nicht statt
- **IT und OT** müssen gleichermaßen berücksichtigt werden

Das definierte Ziel

Mögliche **Schwachstellen** der IT des Unternehmens sollten in einer Außensicht genauso wie aus der Innensicht erfahrbar gemacht werden. Zudem sollten neben der internen IT auch externe Systeme und deren Sicherheit in den Test mit einbezogen werden.

Die Umsetzung

- Initialer **Blackbox Pentest**
- Identifikation von Angriffsvektoren
- Akribische Dokumentation der Ergebnisse
- Beratung bzgl. möglicher **Reformen der IT-Sicherheit**
- Konsequente Schaffung weiterer **Kapazitäten für IT- und OT-Sicherheit**

Zusammenfassung

Immer mehr IT-Services werden heute digital abgebildet und IT-Systeme sind stark miteinander verwoben. Dieses zusätzliche Wachstum sowie die sich abzeichnenden Abhängigkeiten sorgen für mehr potenzielle Schwachstellen in der IT-Infrastruktur. Der Bitkom definiert den Begriff IT-Resilienz als die „Fähigkeit, eine innere Widerstandsfähigkeit gegenüber Krisen und Belastungen zu zeigen." Das trifft auf die ganze Organisation zu, nicht nur auf partielle technische Systeme.

Beispielhafte Bereiche, die es bezüglich einer konsistenten Strategie zur IT-Resilienz zu beachten gilt, sind unter anderem die folgenden: **Software, IT-Sicherheit und Datenschutz, konsequente & kontinuierliche Schulung von Mitarbeitenden und die sachgerechte Skalierung von Arbeitsprozessen hinsichtlich hybridem Arbeiten.**

Der Aufbau einer Infrastruktur, die als resilient in Erscheinung tritt, sollte dabei nicht als Problem, sondern vielmehr **als Chance** wahrgenommen werden. Die vorgenommenen Veränderungen können zu großen **Effizienzschüben** durch einfachere Prozesse und eine geringere Ressourcenbindung führen und unterstützen oft aktuelle Trends, wie bspw. modernste Sicherheitstechniken oder das Arbeiten im Homeoffice.

Bei der IT-Resilienz ist es empfehlenswert eine **Priorisierung der vorhandenen Szenarien** durchzuführen. Denn kritische Geschäftsprozesse oder Infrastrukturen und respektive IT-Systeme besitzen einen deutlich höheren Schutzbedarf und entsprechende Anforderungen an die Widerstandsfähigkeit.

Sie wollen mehr erfahren? Kontaktieren Sie uns.

Wir helfen Ihnen gern und unterstützen Sie von der Idee bis zur Umsetzung. Desweiteren setzen wir uns als erfolgreicher Enabler für den langfristigen Transfer von Wissen innerhalb Ihres Unternehmens ein.

Die Assecor-Gruppe gestaltet digitale Zukunft ganzheitlich. Ein essenzieller Teil der Gruppe ist die Assecor GmbH, eine inhabergeführte, mittelständische IT-Beratung sowie Softwareentwicklungsfirma aus Berlin mit weiteren Standorten in Stralsund und Nürnberg. Seit nunmehr 15 Jahren ist Assecor erfolgreich bei Enterprise- und Mittelstandskunden in verschiedenen Branchen tätig.
Als Cybersecurity-Dienstleister ist Splone ebenfalls Teil der Assecor-Gruppe. Mit ihrer Expertise in Sachen Pentesting und IT-Resilienz erweitert Splone das Leistungsspektrum ungemein.

www.assecor.de
www.splone.com

Ihre Ansprechpartner für konkrete Fragen zum Thema Pentesting und IT-Resilienz:

Hinnerk de Boer
sales@assecor.de

Sascha Zinke
sascha.zinke@splone.com

ASSECOR

Storkower Str. 207 / 10369 Berlin
T: +49 30 233 200 200
info@assecor.de
www.assecor.de

splone

Storkower Str. 207 / 10369 Berlin
T: +49 30 233 200 200
info@assecor.de
www.splone.com