Norbert Pohlmann

Die Notwendigkeit von neuen IT-Sicherheitskonzepten

IT-Sicherheit lässt sich aus zwei Perspektiven betrachten: die der Verteidiger sowie der Angreifer. Erstere ergreifen Maßnahmen, um diese zu schützen – das Ziel letzterer besteht darin, diese überwinden. Doch Fakt ist, dass hier ein Ungleichgewicht herrscht, denn professionelle Angreifer können momentan sehr erfolgreich agieren. Dies lässt sich in erster Linie darauf zurückführen, dass Unternehmen allgemein (noch) nur ungenügend gesichert sind – die aktuell genutzten IT-Sicherheitsmechanismen sind durchweg insgesamt nicht wirkungsvoll genug, um einen angemessenen Schutz zu bieten. Hier muss sich etwas ändern, denn die durch einen erfolgreichen Angriff verursachten Schäden können Unternehmen existenziell gefährden. Neue IT-Sicherheits-Paradigmen wie Zero Trust werden helfen, Unternehmen besser zu schützen.

1 Die IT-Sicherheitslage im Cyberraum

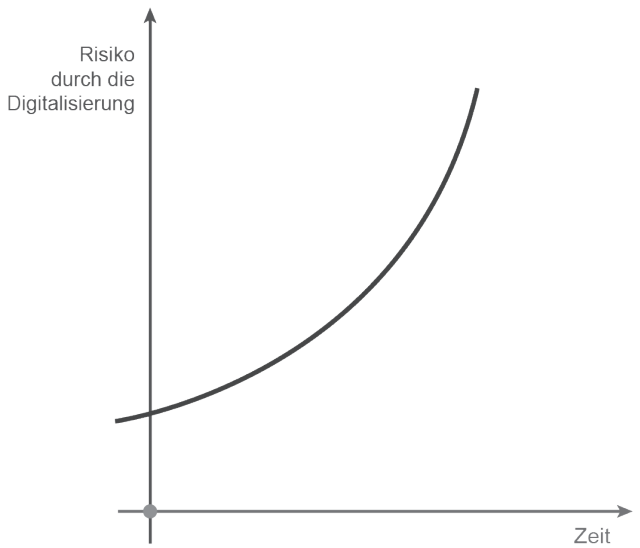
Die IT-Sicherheitslage im Cyberraum wird jedes Jahr gravierender, das bedeutet, dass das Risiko eines Schadensfalls für alle Unternehmen und Organisationen steigt (siehe die rote Kurve, Abbildung 1). Obwohl kontinuierlich bis heute neue IT-Sicherheitstechnologien wie Firewall, VPN, IDS und Vertrauensdienste entwickeln wurden, ist es bislang nicht gelungen der negativen Entwicklung entgegenzuwirken. Das Resümee aus dieser Beobachtung kann nur lauten, dass grundlegend etwas bei den eingesetzten IT-Sicherheitsmechanismen geändert werden muss, um diesen Verlauf zu stoppen und so die digitale Zukunft umsetzen zu können.

Die Gründe für die IT-Sicherheitslage im Cyberraum sind vielfältig. Zum einen sind die IT-Systeme und -Infrastrukturen weder sicher genug konzipiert, aufgebaut, konfiguriert noch bedarfsgerecht upgedatet, um intelligenten Angriffen Stand zu halten.

Nicht sicher genug konzipiert und aufgebaut bedeutet, dass die meisten IT-Systeme mit sehr großen monolithischen Betriebssystemen arbeiten, die keine sichere und vertrauenswürdige Basis darstellen, weil sie zu komplex sind und dadurch zu viele Schwachstellen beinhalten. Schlecht konfiguriert meint zum Beispiel, das viel zu viel Software auf den IT-Systemen installiert ist, die nicht benötigt wird, doch – aus Sicht der Angreifer – einen guten Angriffspunkt bieten, ebenso wie Überberechtigungen. Nicht bedarfsgerecht upgedatet stellt unter dem Aspekt ein großes Gefahrenpotential dar, da zu oft entweder überhaupt nicht oder nicht rechtzeitig Updates einspielt werden, um bekanntgewordene Schwachstellen zu schließen und so Angreifern ermöglicht wird diese unmittelbar professionell ausnutzen.

Ein weiterer Sicherheitsaspekt ist, dass IT-Systeme und -Infrastrukturen insgesamt mit der fortschreitenden Digitalisierung

Abb. 1 | Risiko durch die Digitalisierung



Norbert Pohlmann

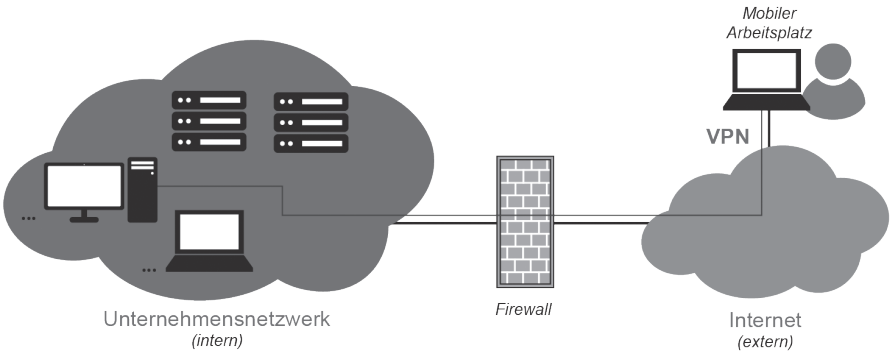
ist Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit TeleTrusT und im Vorstand des Internetverbandes – eco.
E-Mail: pohlmann@internet-sicherheit.de

zunehmend komplexer werden und sich dadurch Angriffsfläche für Angreifer vergrößert. Zudem binden IT-Lösungen vermehrt fremde Software und Dienstleistungen im Sinne von Supply Chains ein, die oft weder sicher noch vertrauenswürdig genug sind.

Ein zusätzlicher Risiko-Faktor ist, dass die Angriffsmethoden der Angreifer immer ausgefeilter werden, weil die Angreifer in kriminellen Ökosysteme organisiert sind. Diese Ökosysteme werden sehr professionell betrieben und sind sehr erfolgreich, das heißt erwirtschaften momentan sehr hohe Gewinne zum Beispiel mit Ransomware-Angriffen. Diese Gewinne werden in zunehmend ausgefeilte sowie automatisierte Angriffstools re-investiert. Damit steigt zum einen die Wahrscheinlichkeit bei jedem Angriff diesen erfolgreich durchführen zu können und zu anderen erweitert sich durch den Einsatz umfänglich automatisierter Tools das Angriffspotential, da auch kleinere Unternehmen zunehmend effektiver angegriffen.

Positiv für den Angreifer aber negativ für den Anwender ist, dass die Angriffsziele aufgrund der zunehmenden Digitalisierung kontinuierlich lukrativer werden, da sich immer mehr digitale Werte auf den IT-Systemen befinden. Auch wenn die Risiko-Faktoren hier nicht abschließend dargestellt werden können, zeigt sich doch, dass die Risiken steigen und Unternehmen deutlich wirkungsvollere IT-Sicherheitsmechanismen benötigen, um sich im Rahmen der digitalen Transformation angemessen zu schützen.

Abb. 2 | Perimeter-Sicherheit



2 IT-Sicherheits-Paradigma: Perimeter-Sicherheit

Die Perimeter-Sicherheit ist ein traditionell verwendetes Sicherheitsmodell oder auch eine IT-Sicherheitsstrategie. Die Idee ist, eine Netzwerk-Unterteilung in intern und extern vorzunehmen. Intern ist das Unternehmensnetzwerk und extern ist das Internet, siehe Abbildung 2.

Der Fokus wird auf den Schutz vor externen Angriffen gelegt – durch Abschottung und Abgrenzung. Dazu werden in der Regel Firewall, Intrusion Detection Systems (IDS) sowie weitere zentrale Filter wir zum Beispiel im Bereich Malware oder Spam umgesetzt [1]. Der Zugang von mobilen und Heim-Arbeitsplätzen zum internen Unternehmensnetzwerk wird in der Regel mittels VPN realisiert. In der Theorie stehen alle IT-Systeme im vertrauenswürdigen Netz (grünes Netz) und nur vertrauenswürdige Mitarbeiter des Unternehmens haben einen Zugriff auf die internen IT-Systeme. Der Zugang zum Internet geht in der Theorie nur über die Firewall. Die IT-Sicherheit im internen Netz und deren IT-Systemen ist in der Regel eher gering, weil das Unternehmensnetzwerk als vertrauenswürdig eingestuft wird.

2.1 Probleme mit der Perimeter-Sicherheit

Ein Grund für die Unzulänglichkeit der Perimeter-Sicherheit sind die modernen Arbeitsweisen und -methoden wie Homeoffice, Cloud Computing und Bring-your-own Device (BYOD), da hier die Grenzen nicht mehr eineindeutig definiert werden können.

Ein weiteres Problem ist, sobald ein Angreifer in das interne Netz eingedrungen ist, hat dieser leichtes Spiel, weil die IT-Sicherheit wegen dem Paradigma „Perimeter-Sicherheit“ nicht so stark ausgeprägt ist.

2.1.1 Problem VPN-Zugang

Im Folgenden wird ein typischer Angriffsvektor beschrieben, der bei vorhandenen VPN-Zugängen durch kriminelle Organisationen wie zum Beispiel bei Ransomware-Angriffen zurzeit sehr erfolgreich umgesetzt wird. Der Angreifer schaut sich in Business-Netzwerken wie LinkedIn oder Xing um, damit er weiß, wer der Administrator in einem bestimmten Unternehmen ist und welche Hobbies oder Vorlieben der Administrator hat. Diese Informationen werden dazu genutzt, um über eine ansprechende Spear-Phishing-Mail den Administrator zu motivieren, auf einen Link oder einen Anhang zu klicken. Dadurch bekommt der Administrator eine Malware auf sein IT-System installiert. Mithilfe dieser Malware kann der Angreifer durch die Firewall und den Rechten des Administrators auf ein erstes internes IT-System zugreifen. Dort richtet sich der Angreifer ein und verwischt seine bisherigen Spuren. Anschließend organisiert er sich in aller Ruhe mit weiteren intelligenten Angriffstools zusätzliche Rechte auf anderen IT-Systemen in Unternehmensnetzwerk.

Mit diesen Rechten kann der Angreifer umfangreiches Wissen, Schwachstellen und Werte auf den IT-Systemen des Unternehmens sammeln und die Gewalt über alle IT-System erlangen. Wenn er genug Informationen generiert und ausreichend IT-Systeme übernommen hat, werden die Informationen aus dem Unternehmen abgezogen und im nächsten Schritt alle IT-Systeme verschlüsseln, um so den Stillstand der kompletten IT eines Unternehmens zu initiieren. Anschließend können die Angreifer eine Lösegeldforderung für die Herausgabe des Schlüssels stellen, mittels dessen der Wiederanlauf des Betriebs ermöglichen werden soll.

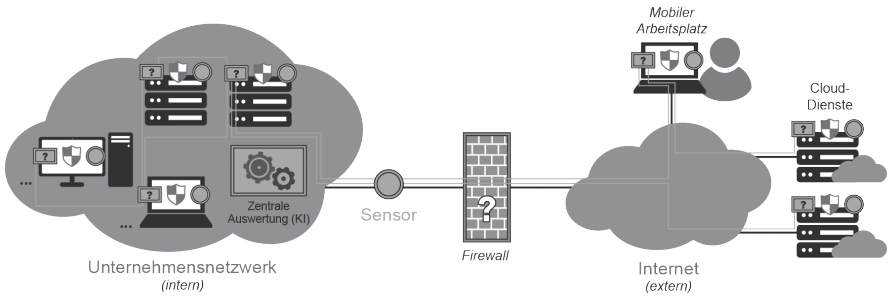
Wenn zum Beispiel 3.000 Mitarbeiter vor der Türe stehen und nicht reinkommen, weil die moderne IT-Schließanlage nicht mehr funktioniert, die Kunden und Lieferanten nicht informieren werden können, weil die Telefonnummern und E-Mail-Adressen auf den nicht mehr verfügbaren IT-Systemen stehen, ist die Wahrscheinlichkeit sehr hoch, dass das Lösegeld schnell bezahlt wird, weil jeder Tage Ausfall sehr viel Geld kostet und einen Reputationsschaden verursacht.

2.1.2 Bring-Your-Own-Device – BYOD-Geräte

Bring-your-own-Device (BYOD) erlaubt es Mitarbeitenden, Kunden, externen Dienstleistern und Partnern private Geräte wie Smartphones und Notebooks im Unternehmensnetzwerk zu nutzen.

Doch diese BYOD-Geräte können, da sie oft unterwegs genutzt werden, leichter angegriffen werden – zum Beispiel, wenn die Mitarbeitenden in einer öffentlichen Umgebung wie Cafés, Hotels oder Flughäfen ein unverschlüsseltes WLAN nutzen. Wenn sie sich dann mit diesem infizierten Gerät in das interne Unternehmensnetzwerk einwählen, wird die Malware an der zentralen Firewall vorbei direkt eingeschleust – im Prinzip der gleiche Angriff wie über den VPN-Zugang. Des Weiteren nutzen Mitarbeiter alternative Kommunikationswege wie Mobilfunknetze an der zentralen Unternehmens-Firewall vorbei für ihren Zugang ins Internet. Auch dadurch können Angreifer, an der Firewall vorbei, in das interne Unternehmensnetz gelangen, sodass die Perimeter-Sicherheit hier an Wirkung und Bedeutung verliert.

Abb.3 | Zero Trust-Konzept



2.1.3 Cloud-Dienste

Im Rahmen der Perimeter-Sicherheit gilt es die Cloud-Dienste besonders zu betrachten, da diese in der Regel nicht durch den eigentlichen Perimeter des Unternehmens geschützt werden.

2.1.4 Interne Angriffe

Bei der Perimeter-Sicherheit werden IT-Sicherheitsdienste zur Abschottung gegen das unsichere Netz oder zur Kontrolle der Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz angeboten. Bezüglich interner Angriffe stehen in der Regel keine IT-Sicherheitsmaßnahmen zur Verfügung.

2.2 Bewertung der Perimeter-Sicherheit

Die Idee von Perimeter-Sicherheit war zu Beginn des Internets eine sehr gute IT-Sicherheitsarchitektur. Aber die Perimeter-Sicherheit hat durch die Veränderung der Arbeitsweise sowie intelligente Angriffsmethoden deutlich an Wirkung und damit an Bedeutung verloren. Daher werden sehr wirksame IT-Sicherheitsmechanismen benötigt, um die IT-Systeme der Unternehmen und Organisationen in der zunehmenden Digitalisierung wirkungsvoll zu schützen.

Dazu muss die IT-Sicherheitsarchitektur neu gedacht und umgesetzt werden.

3 IT-Sicherheits-Paradigma: Zero Trust Konzept

Die Grundidee bei Zero Trust lautet: „**Vertraue nie, überprüfe immer**“

Beim Zero Trust-Prinzip wird nichts und niemandem vertraut, weder dem IT-System noch einem Nutzer, IT-Dienst, Netzwerk und ebenfalls weder IT-Anwendungen noch IT-Prozessen, IT-Infrastruktur – allgemein IT-Entität – innerhalb oder außerhalb des „eigenen Netzwerks“.

Das bedeutet, sämtliche Kommunikation zwischen den IT-Entitäten wird kontrolliert, reglementiert sowie auf Angriffsversuche untersucht. Zudem werden alle IT-Entitäten robust aufgebaut und müssen sich gegenseitig authentifizieren. Dazu ist es notwendig, dass alle IT-Entitäten eine eindeutige digitale Identität haben.

Auf der Basis von verschiedenen, aber ineinander wirkenden IT-Sicherheits- und Vertrauenswürdigkeitsmechanismen soll durch Zero Trust die Angriffsfläche der eigenen IT-Landschaft so klein wie möglich gehalten und die Robustheit der IT-Systeme deutlich größer werden.

Bei Zero Trust gibt es einige Modelle und Frameworks, die bei der Umsetzung betrachtet werden können. Diese Modelle und Frameworks beschreiben dabei einige für Zero Trust relevante Maßnahmen. Ein erstes Modell ist BeyondCorp, das Zero Trust Modell von Google, was 2011 vorgestellt worden ist [2]. Im Jahr 2018 wurde von Forester das Zero Trust eXtended (ZTX) Ecosystem ins Leben gerufen [3]. Im Jahr 2020 publizierte das National Institute of Standards and Technology (NIST) ein Paper zum Thema Zero Trust [4]. Im Mai 2021 veröffentlichte das Weiße Haus die „Executive Order on Improving the Nation’s Cybersecurity“ [5]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte ein Positionspapier im Juni 2023 [6].

3.1 Prinzipielle Umsetzung eines Zero Trust Konzeptes

Prinzipiell kann ein Zero Trust-Konzept wie folgt umgesetzt werden. In Abbildung 3 ist erkennbar, dass das interne Unternehmensnetz nicht mehr als vertrauenswürdig eingeschätzt wird (graues Netz). Das bedeutet, dass alle IT-Systeme des Unternehmens selbst so sicher und robust aufgebaut, konfiguriert sowie gemanagt werden müssen, dass es nicht möglich ist, diese erfolgreich anzugreifen.

3.2 Notwendige IT-Sicherheitsmechanismen

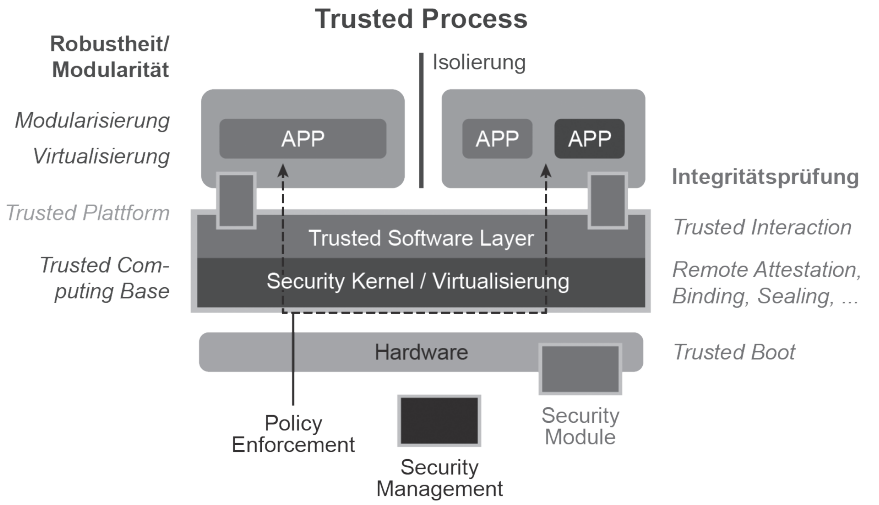
Im Folgenden werden einige wichtige IT-Sicherheitsmechanismen beschrieben, mit denen die Zero Trust-Idee umgesetzt werden kann.

3.2.1 Alle Netzteilnehmer (IT-System, IT-Entität, Nutzer) müssen sich gegenseitig authentifizieren

Damit die Netzteilnehmer wissen, mit wem sie in Interaktion stehen, müssen sie sich gegenseitig authentifizieren. Die Authentifi-

kationsmethode sollte mit einem Faktor auf Basis von starken kryptografischen Verfahren aufgebaut sein. Diese Anforderung ist nicht trivial, weil das übergreifend für alle IT-Systeme verschiedener Hersteller funktionieren muss. Dazu wird ein herstellerübergreifendes Management-System benötigt, dass einem breit eingesetzten Standard genügt.

Abb. 4 | Trusted Computing Sicherheitsarchitektur



3.2. 2 Minimalen Rechte auf allen IT-Entitäten (Least-Privilege-Prinzip)

Jedes nicht notwendige Recht auf einer IT-Entität schafft prinzipiell die Möglichkeit, einen Angriff umzusetzen. Daher muss das Ziel sein, durch die Vermeidung von Überberechtigungen die Angriffsfläche und damit eine Reduzierung der Risiken zu erreichen. Die Herausforderung besteht darin, minimale Rechte auf allen IT-Entitäten so einzurichten, dass das Unternehmen alle erforderlichen Prozesse für die Geschäftstätigkeit umsetzen kann, aber alles andere aktiv vermieden wird.

3.2.3 Moderne End-Point-Security

Es wird ein modernes End-Point-Sicherheitssystem, das dem Stand der Technik genügt – das heißt die am Markt verfügbare Bestleistung darstellt – eingesetzt. Dieses muss intelligente Sicherheitssensoren in allen IT-Systemen/-Entitys sowie in der Kommunikation aufweisen. Die hier entstehenden sicherheitsrelevanten Informationen müssen an eine zentrale KI-Auswertung gesendet werden, um in einer zentralen Auswertung globale Sichtweisen aufzubauen, wodurch es sehr viel einfacher sowie schneller möglich ist Angriffe zu erkennen.

3.2.4 Automatische Reaktionen

Zudem werden automatische Reaktionsmechanismen benötigt, die das Eindringen von Malware stoppen können, IT-Systeme isolieren, wenn sie verseucht sind oder Regeln von Firewall, E-Mail-Server oder andere Komponenten reduzieren, um die Angriffsfläche in einem Angriffsfall schnell zu reduzieren.

3.2.5 Verschlüsselte Kommunikation

Sämtliche Kommunikationen zwischen den IT-Entitäten ist verschlüsselt und Integrität-gesichert. Im Kontext der Verschlüsselung gibt es einen sehr hohen Nachholbedarf, doch da diese ein sehr wirkungsvoller IT-Sicherheitsmechanismus zum Schutz der Daten und IT-Entitäten ist, gilt es hier konsequent Verschlüsselung überall umzusetzen.

3.2.6 Robustheit der IT-Systeme

Damit alle IT-Systeme sicher und vertrauenswürdig umgesetzt werden können, werden moderne und intelligente IT-Sicherheitsarchitekturen, -konzepte und -funktionen benötigt, mit denen eine höheren Robustheit und ein höherer IT-Sicherheitslevel umgesetzt werden kann.

Mit der Hilfe von Trusted Computing werden zum Beispiel eine IT-Sicherheits- und Vertrauenswürdigkeitstechnologie angeboten, mit denen einige große IT-Sicherheitsprobleme wie Softwarefehler und Malware in ihrer Wirkung deutlich eingeschränkt werden können.

3.3 Prinzipieller Aufbau einer Trusted Computing Sicherheitsarchitektur

In der Abbildung 4 sind die Sicherheitsprinzipien und -mechanismen sowie der prinzipielle Aufbau einer Trusted Computing Sicherheitsarchitektur dargestellt.

Im Folgenden werden die Sicherheitsprinzipien und -mechanismen der Trusted Computing Sicherheitsarchitektur dargestellt.

3.4 Robustheits- und Modularitätsaspekte

3.4.1 Trusted Computing Base (TCB)

Eine „Trusted Computing Base" dient als verlässliches Fundament, um darauf weitere Komponenten aufzubauen. Per Definition ist die „Trusted Computing Base" der kritische Teil eines IT-Systems. Wenn im TCB eine Schwachstelle vorhanden ist, dann ist das ganze IT-System kompromittiert. Wenn außerhalb der TCB eine Schwachstelle vorhanden ist, dann kann anhand einer Sicherheitspolicy der potenzielle Schaden sehr eingeschränkt und klar beschrieben werden. Aus diesem Grund ist eine TCB sehr sorgfältig designt und implementiert. Eine auf einem Mikrokernel (Security Kernel) basierende TCB hat ca. 20.000 Lines of Code und ist aus diesem Grund eine sehr vertrauenswürdige Basis, die in der Regel auch schon semiformal oder formal verifiziert werden kann. Mithilfe der formalen Beweisbarkeit wird eine Sicherheitsevaluation auf hohem Niveau möglich. Es gibt aber auch TCBs, die zum Beispiel aus einem sehr abgespeckten und speziell gehärteten Linux bestehen, das auch schon sehr viel vertrauenswürdiger ist als übliche Betriebssysteme.

3.4.2 Virtualisierung

Ein weiterer wichtiger Sicherheitsaspekt ist die Virtualisierung auf dem IT-Systeme. Der Vorteil von Virtualisierung besteht darin, dass auftretende Fehler (Schwachstelle, Malware …) in einer virtuellen Maschine in einem abgeschlossenen Bereich begrenzt bleibt und nicht eine andere virtuelle Maschine infizieren kann. Es ist auch sehr einfach möglich, die verschiedenen virtuellen Maschinen wieder in einen stabilen Urzustand zu versetzen und von da aus neu zu starten.

3.4.3 Isolierung

Der Sicherheitsaspekt Isolierung sorgt dafür, dass die virtuellen Maschinen zusätzlich weiter stark isoliert und sicher getrennt voneinander laufen und sich nicht gegenseitig beeinflussen können und daher Schwachstellen und „Angreifer" in einer isolierten virtuellen Maschine keinen Einfluss auf die anderen virtuellen Maschinen hat.

3.4.4 Modularisierung

Der Sicherheitsaspekt der Modularisierung ist eine Möglichkeit, Anwendungen, die zusammengehören, in einer virtuellen Maschine laufen zu lassen und Anwendungen, die getrennt sein sollten, in verschiedenen virtuellen Maschinen zu positionieren. Dieser Sicherheitsaspekt offeriert einen interessanten Gestaltungsspielraum, mit dem eine sehr hohe IT-Sicherheit erzielt werden kann, weil für verschiedene Sicherheitslevel von Anwendungen unterschiedliche virtuelle Maschinen genutzt werden können. Ein Beispiel ist: Das Office-Paket läuft in einer virtuellen Maschine, das Design-Paket für die Business-Anwendung in einer anderen und der Browser hat auch eine separate virtuelle Maschine.

3.5 Sicherheitsaspekt Integritätsüberprüfung

Der Sicherheitsaspekt Integritätsüberprüfung wird genutzt, um den vertrauenswürdigen Zustand eines IT-Systems überprüfen zu können.

3.5.1 Trusted Software Layer

Die Trusted Software Layer stellt dazu vertrauenswürdige Sicherheitsdienste zur Verfügung, die helfen, IT-Systeme (Hardware, Software und Konfigurationen) vertrauenswürdig zu gestalten und messbar zu machen.

3.5.2 Security Module (TPM)

Das Security Module (Hardware-Sicherheitsmodul) ist zum Beispiel ein TPM mit intelligenten kryptografischen Verfahren auf dem Level von Smartcard-Sicherheit, aber auch weiteren Sicherheitsdiensten wie die Platform Configuration Register (PCR), die die sichere Speicherung und Überprüfung von Messdaten sicherstellt. Das TPM ist ein kleiner passiver Hardware-Sicherheitschip, der fest mit dem Mainboard verbunden ist. Damit steht prinzipiell ein Hardware-Sicherheitsmodul auf jedem IT-Systemen zur Verfügung.

Vorteile eines TPMs: Die Hardware-Sicherheitsmodule bieten eine sehr hohe IT-Sicherheit bei geringer Investitionssumme, da ein TPM nicht mehr als ein Euro kostet. Die Hardware-Sicherheitsmodule sind schon auf dem überwiegenden Teil der IT-Systeme verfügbar, das heißt, die flächendeckende Einführung einer Sicherheitsplattform ist einfach! Wenn ein IT-System „Microsoft Ready" sein soll, muss es ein TPM verbaut haben. Die Hardware-Sicherheitsmodule sind in eine Sicherheitsinfrastruktur (PKI …) eingebunden und daher einfach im Sicherheitsmanagement zu behandeln.

3.5.3 Trusted Boot/Authenticated Boot

Mithilfe von Trusted Boot oder Authenticated Boot ist es möglich dafür zu sorgen, dass ein IT-System nur in einem definierten vertrauenswürdigen Zustand aktiv wird.

3.5.4 Remote Attestation

Remote Attestation gibt die Möglichkeit, die Vertrauenswürdigkeit von anderen, auch fremden IT-Systemen zu messen, bevor eine Interaktion mit diesem IT-System begonnen wird.

3.5.5 Binding/Sealing

Binding und Sealing sind weitere Trusted Computing-Funktionen, mit denen moderne IT-Sicherheitssystem intelligent und vertrauenswürdig umgesetzt werden können. Bei Binding werden verschlüsselte Daten an ein TPM gebunden. Bei Sealing werden verschlüsselte Daten an die Software- und Hardware-Konfiguration eines IT-Systems sowie an ein TPM gebunden.

3.5.6 Trusted Interaction

Unter dem Begriff „Trusted Interaction" werden Sicherheitsdienste in den Trusted Software Layern zusammengefasst, die dafür sorgen, dass Informationen vertrauenswürdig eingegeben, gespeichert, übertragen und dargestellt werden können.

3.6 Sicherheitsaspekt Trusted Process

Trusted Prozess vereint die Sicherheitsaspekte, die die Abläufe in den und mit den verschiedenen IT-Systemen betreffen.

3.6.1 Security Management

Security Management fasst die wichtigen Funktionen zusammen, die notwendig sind, um das proaktive Sicherheitssystem vertrauenswürdig nutzbar zu machen.

3.6.2 Policy Enforcement

Mithilfe des Policy Enforcements ist eine Trusted Plattform in der Lage, die definierte Regel auf dem eigenen, aber auch auf fremden IT-Systemen vertrauenswürdig umzusetzen.
Durch die Kombination und das Zusammenwirken aller Sicherheitsaspekte stellt Trusted Computing die vertrauenswürdige Basis dar, die für die Umsetzung von sicheren und robusten IT-Systemen im Zero Trust Konzept ideal genutzt werden kann.

4 Zusammenfassung

Um vor intelligenten Angriffen, die heute sehr erfolgreich durchgeführt werden, zu schützen, sind traditionelle Sicherheitsarchitekturen wie die Perimeter-Sicherheit nicht mehr ausreichend. Es werden moderne IT-Sicherheits-Architekturen benötigt.

Der Zero Trust-Ansatz ist sehr gut geeignet, dass Unternehmen sich gegen intelligente Angriffe angemessen schützen können.

Doch die Umsetzung birgt verschiedene Herausforderungen. Aus diesem Grund wird es nicht möglich sein Zero Trust von jetzt auf gleich umzusetzen. Im Gegenteil – um das Ziel einer angemessen IT-Sicherheit zu erreichen bedarf es einer gut geplanten Vorgehensweise, mittels deren in kleinen Schritten dafür gesorgt wird, dass die Angriffsfläche kontinuierlich minimiert und die Robustheit aller IT-Systeme deutlich vergrößert wird.

Literatur

[1] N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer-Vieweg Verlag, Wiesbaden 2022

[2] BeyondCorp Zero Trust Enterprise Security | Google Cloud: in: Google Cloud, o. D., [online] https://cloud.google.com/beyondcorp (abgerufen am 30.11.2023)

[3] S. Turner, C. Cunningham, J. Blankenship, S. Balaouras, R. Murphy, A. Bouffard, P. Dostie: “The Zero Trust eXtended (ZTX) Ecosystem”, in: Forrester, 23.08.2021, [online]

[4] K. Alper: ”Zero Trust Cybersecurity: ‘Never trust, always verify’”, NIST, in: NIST, 29.11.2022, [online] https://www.nist.gov/blogs/taking-measure/zero-trustcybersecurity-never-trust-always-verify.

[5] Cybersecurity and Infrastructure Security Agency: Zero Trust Maturity Model, 04.2023, [online] https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (abgerufen am 30.11.2023).

[6] Bundesamt für Sicherheit in der Informationstechnik: Positionspapier Zero Trust 2023, 26.06.2023, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-undOrganisationen/Informationen-und-Empfehlungen/Zero-Trust/zero-trust.html (abgerufen am 30.11.2023)