Jason Garbis
Jerry W. Chapman

Zero Trust Sicherheit

Ein Leitfaden für Unternehmen

Springer Vieweg

Zero Trust Sicherheit

Ein Leitfaden für Unternehmen

Jason Garbis
Jerry W. Chapman

Apress®

Zero Trust Sicherheit: Ein Leitfaden für Unternehmen

Jason Garbis
Boston, MA, USA

Jerry W. Chapman
Atlanta, GA, USA

ISBN 979-8-8688-0104-4 ISBN 979-8-8688-0105-1 (eBook)
https://doi.org/10.1007/979-8-8688-0105-1

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der DeutschenNationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Übersetzung der englischen Ausgabe: „Zero Trust Security“ von Jason Garbis und Jerry W. Chapman, © Jason Garbis and Jerry W. Chapman 2021. Veröffentlicht durch Apress. Alle Rechte vorbehalten.

Dieses Buch ist eine Übersetzung des Originals in Englisch „Zero Trust Security“ von Jason Garbis, publiziert durch APress Media, LLC im Jahr 2021. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

Planung/Lektorat: Susan McDermott
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft APress Media, LLC und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: 1 New York Plaza, New York, NY 10004, U.S.A.

Das Papier dieses Produkts ist recycelbar.

Für Amy, Shira und Shelly
—J.G.

Für meine schöne und liebevolle Frau, Suzette—Danke!
An unsere geliebten Töchter, Nena und Alex—Ihr seid geliebt!
—J.W.C.

Inhaltsverzeichnis

Über die Autoren

Jason Garbis ist Gründer und Leiter von Numberline Security, einem Beratungsunternehmen, das Schulungen und Beratungsdienste zu Zero Trust Security anbietet. Jason ist Mitautor des viel beachteten Buches „Zero Trust Security: An Enterprise Guide“, Co-Vorsitzender der Zero Trust Working Group bei der Cloud Security Alliance und ist ein häufiger Redner auf Branchenkonferenzen. Jason ist CISSP-zertifiziert, hat einen BS in Computerwissenschaften von Cornell und einen MBA von Northeastern. Beruflich hat er Erfahrung in den Bereichen Identitätsmanagement, Unternehmenssicherheitsarchitekturen, Netzwerksicherheit und Sicherheitsstrategie. Zuvor war er als Chief Product Officer bei Appgate tätig und hatte Positionen bei Sicherheitsunternehmen wie RSA und Aveksa inne.

Jerry W. Chapman ist ein Cybersecurity-Experte mit Schwerpunkt Identität. Mit mehr als 25 Jahren Branchenerfahrung hat Jerry Chapman zahlreiche Kunden erfolgreich bei der Konzeption und Implementierung ihrer Unternehmens-IAM-Strategien beraten, die sowohl den Sicherheits- als auch den Geschäftszielen entsprechen. Seine Aufgaben umfassten die Bereiche Unternehmensarchitektur, Solution Engineering sowie Softwarearchitektur und -entwicklung. Jerry ist Co-Vorsitzender der Zero Trust Working Group bei der Cloud Security Alliance und ist in der technischen Arbeitsgruppe der Identity Defined Security Alliance (IDSA) aktiv, wo er der ursprüngliche Technical Architect der Gruppe war. Jerry ist ein zertifizierter Forrester Zero Trust Strategist, hat einen BS in Computer Information Systems von

der DeVry University und macht derzeit einen Abschluss in angewandter Mathematik von der Southern New Hampshire University.

Über den technischen Gutachter

Christopher Steffen bringt über 20 Jahre Branchenerfahrung als bekannter Informationssicherheitsleiter, Forscher und Präsentator mit, mit Schwerpunkt auf IT-Management/Führung, Cloud-Sicherheit und regulatorischer Konformität.

Chris hatte eine Vielzahl von Rollen als Fachmann und/oder Führungskraft, vom Campingdirektor für die Pfadfinder bis zum Pressesekretär für den Sprecher des Hauses in Colorado. Seine technische Karriere begann im Finanzdienstleistungssektor in der Systemverwaltung für ein Kreditberichtsunternehmen, baute schließlich die Netzwerkbetriebsgruppe auf, sowie die Praxis für Informationssicherheit und technische Compliance für das Unternehmen, bevor er als Haupttechnischer Architekt ausschied. Er war der Direktor für Information bei einem Produktionsunternehmen und der Chief Evangelist für mehrere technische Unternehmen, mit Schwerpunkt auf Cloud-Sicherheit und Cloud-Anwendungstransformation, und hatte auch die Position des CIO eines Finanzdienstleistungsunternehmens inne, bei dem er die technologiebezogenen Funktionen des Unternehmens überwachte.

Chris ist derzeit der leitende Forscher für Informationssicherheit, Risiko- und Compliance-Management bei Enterprise Management Associates (EMA), einem führenden Branchenanalystenunternehmen, das tiefe Einblicke in das gesamte Spektrum der IT- und Datenmanagementtechnologien bietet.

Chris besitzt mehrere technische Zertifizierungen, einschließlich Certified Information Systems Security Professional (CISSP) und Certified Information Systems Auditor (CISA), und wurde fünfmal mit dem Microsoft Most Valuable Professional Award für Virtualisierung und Cloud- und Data Center Management (CDM) ausgezeichnet. Er hat einen Bachelor of Arts (Summa Cum Laude) vom Metropolitan State College of Denver.

Danksagungen

Zero Trust-Sicherheit umfasst ein sehr breites Gebiet, und der Prozess, den wir durchlaufen haben, um technische, nicht-technische und architektonische Konzepte zu erkunden, zu lernen und zu verknüpfen, war oft herausfordernd. Wir hatten das Glück, viele Menschen zu haben, die bereit waren, Zeit mit uns zu verbringen, uns zu unterrichten, unsere Fragen zu beantworten und Feedback und Anleitung zu geben. Einige Leute halfen uns, indem sie unseren geplanten Entwurf oder unsere Arbeit im Gange lasen und kommentierten, einige trugen dazu bei, indem sie mit uns in Videokonferenzen brainstormten (ein Markenzeichen von 2020, vermuten wir), während andere uns halfen (ob sie es wissen oder nicht), indem sie Teil der Informationssicherheitsindustrie waren und als Teil ihrer regelmäßigen beruflichen Interaktionen mit uns.

Vielen Dank an Dr. Chase Cunningham für Ihren breiten Brancheneinfluss und Brigadegeneral (a.D.) Greg Touhill für Ihre Unterstützung im Vorwort. Und Dank an Sie beide für Ihre Karrieren im Dienst unseres Landes in militärischen und informationssicherheitsbezogenen Rollen. Wir möchten auch Evan Gilman, Doug Barth, Mario Santana, Adam Rose, George Boitano, Bridget Bratt, Leo Taddeo, Rob Black, Deryck Motielall und Kurt Glazemakers danken. Außerdem ein Dankeschön an das Team der Cloud Security Alliance und seiner SDP Zero Trust Arbeitsgruppe, einschließlich Shamun Mahmud, Junaid Islam, Juanita Koilpillai, Bob Flores, Michael Roza, Nya Alison Murray, John Yeoh und Jim Reavis. Und ein weiteres Dankeschön an Julie Smith und das Identity Defined Security Alliance (IDSA) Team, insbesondere die technische Arbeitsgruppe, die die Identität in der Mitte der Sicherheit hält. Wir möchten auch unseren zu zahlreichen Kollegen für ihre vielen Gespräche und ihre Unterstützung danken, sowie unseren Apress-Editoren Rita Fernando und Susan McDermott für ihre Unterstützung, Ermutigung und Hilfe während dieses Prozesses. Und natürlich ein riesiges Dankeschön an unseren technischen Gutachter, klingendes Brett und Freund Chris Steffen.

Schließlich möchten wir uns bei Ihnen bedanken - als Praktiker oder Führer in der Informationssicherheitsbranche, der jeden Tag daran arbeitet, Ihre Organisation besser abzusichern. Wir hoffen, dass dieses Buch Ihre Arbeit erleichtert. Bitte besuchen Sie uns unter https://ZeroTrustSecurity.guide mit jeglichen Kommentaren oder Vorschlägen und um die Begleitvideoserie dieses Buches anzusehen.

Geleitwort

Zero Trust wurde nicht aus dem Bedürfnis heraus geboren, eine weitere Sicherheitskontrolle oder Lösung zu verkaufen. Es entstand aus dem Wunsch, ein reales Unternehmensproblem zu lösen…Zero Trust konzentriert sich auf Einfachheit und die Realität, wie die Dinge jetzt sind.

—Dr. Chase Cunningham, auch bekannt als „Dr. Zero Trust"

Ich habe über zwei Jahrzehnte auf dieses Buch gewartet und freue mich, seine Ankunft vorzustellen.

Lange vor der kühnen Erklärung des Jericho Forums im Jahr 2004 über eine neue Sicherheitsstrategie mit dem Schwerpunkt „De-Perimeterisierung" waren viele von uns in der nationalen Sicherheitsgemeinschaft zu der Erkenntnis gelangt, dass das Perimetersicherheitsmodell keine tragfähige Sicherheitsstrategie mehr für internetverbundene Systeme und Unternehmen war. Der unersättliche Durst, alles mit dem Internet zu verbinden, die steigenden Kosten und die Komplexität der Sicherheitsschichten und das rasante Tempo des technologischen Wandels brachen das Perimetersicherheitsmodell um uns herum auf. Unser Verteidigung-in-die-Tiefe-Sicherheitsperimeter war ein Deich, der zu viele Lecks aufwies, als dass wir in irgendeiner sinnvollen oder fiskalisch verantwortungsvollen Weise Schritt halten könnten. Die Arbeit des Jericho Forums wies in eine andere Richtung und gab vielen von uns eine neue Hoffnung.

Leider hatten sich, wie Grand Moff Tarkin auf dem Todesstern, viele Sicherheitsprofis und Kommentatoren mit dem Status quo angefreundet und die Vorstellung belächelt, dass ein neuer Ansatz zur Sicherung moderner Unternehmen benötigt wurde. Ein Sicherheitskommentator ging sogar so weit zu sagen, dass das Jericho Forum „das Ziel verfehlt" habe und spottete voraus, dass seine Arbeit wahrscheinlich „auf dem Schrotthaufen unrealisierter Ideen und verschwendeter Anstrengungen enden würde." Ich hoffe, dass er dieses Buch mit einem Hauch von Schuld und Bedauern liest.

Die Arbeit des Jericho Forums war nicht umsonst, aber sie brachte auch nicht sofort Früchte. Nach etwas mehr als 5 Jahren seit der Einführung des Konzepts der „De-Perimeterisierung“ prägte John Kindervag, damals Analyst bei Forrester Research, im Jahr 2010 den Begriff „Zero Trust“ zur Beschreibung des Sicherheitsmodells, dass Organisationen nichts außerhalb oder innerhalb ihrer Perimeter automatisch vertrauen sollten, und stattdessen alles und jedes überprüfen müssen, bevor sie sie mit ihren Systemen verbinden und Zugang zu ihren Daten gewähren.

Für uns im Militär war Zero Trust kein revolutionäres Sicherheitsmodell. Wir hatten es mit physischer Sicherheit während unserer gesamten Karriere praktiziert. Zum Beispiel wurde jede Person am Tor von Sicherheitspersonal begrüßt und musste ordnungsgemäße Identitätsnachweise vorlegen, bevor sie Zugang zur Basis erhielt. Wir praktizierten Segmentierung mit Schutzzonen um das, was wir Priorität A, B und C Ressourcen nannten. Die Fluglinienbereiche waren das Zuhause von Priorität A Vermögenswerten und hatten streng kontrollierten Zugang mit bewaffneten Wachen. Rollenbasierte Eintritte wurden streng kontrolliert und der Einsatz von tödlicher Gewalt gegen diejenigen autorisiert, die die „rote Linie durchbrachen“. Als Leutnant musste ich vier Sicherheitsstufen durchlaufen, bevor ich überhaupt in mein Büro gelangen konnte. Sicherheit war in unserer Kultur, unseren Prozessen und unseren Erwartungen verankert.

Leider fehlte die Technologie, um ein „Zero Trust“-Sicherheitsmodell zum Schutz unserer zunehmend wertvollen und mit dem Internet verbundenen digitalen Vermögenswerte zu implementieren, als meine Generation schrittweise die Informationsnetzwerke des Verteidigungsministeriums aufbaute, während wir ein „Zero Trust“-physisches Sicherheitsmodell befolgten, um unsere wertvollsten Einrichtungen und Waffensysteme zu schützen. Kommerziell erhältliche Werkzeuge waren äußerst komplex und teuer. Zum Beispiel mussten wir einen Vertrag mit einem bekannten Anbieter abschließen, um eine „Akademie“ zu schaffen, nur um unsere bereits hochqualifizierte Belegschaft richtig in die Nutzung ihrer komplexen Netzwerkprodukte einzuschulen. Die Kosten stiegen weiter an, während wir unseren Marsch zur Digitalisierung jeder Funktion fortsetzten, doch der Sicherheitsperimeterdamm um uns herum sprang weiterhin Lecks. Als ich vom Bundesdienst als Chief Information Security Officer der US-Regierung in den Ruhestand ging, war ich zu dem Schluss gekommen, dass die Zero Trust-Sicherheitsstrategie unsere einzige Hoffnung war, unser digitales Ökosystem zu sichern.

XX

Die COVID-19-Pandemie hat einen massiven Wechsel von traditionellen Büroumgebungen zu einem Modell der Heimarbeit angestoßen, das den lang erwarteten Übergang zur Zero Trust-Sicherheitsstrategie beschleunigt hat. Die Illusion des Sicherheitsperimeters wurde durch massive Mobilität, Cloud-Computing, Software-as-a-Service und beispiellose Implementierung von Bring-Your-Own-Device in Organisationen überall zerstört, als sie von traditionellen Unternehmensumgebungen zur heutigen modernen digitalen Realität wechselten. Die Realität heute ist, dass der traditionelle Netzwerksicherheitsperimeter tot ist; es gibt kein „außen“ oder „innen“ mehr.

Leider sind viele Menschen und Organisationen, einschließlich dieses Skeptikers, der die Vision des Jericho Forums verspottet hat, auf den Zero Trust-Zug aufgesprungen. Viele bekennen sich zu „Zero Trust“, wissen aber nicht, was es wirklich ist oder wie man es praktiziert. Organisationen, deren veraltete Netzwerktechnik und -methoden sich als übermäßig komplex und anfällig erwiesen haben, lassen ihre Marketingteams ihre anfälligen Fähigkeiten wunderbarerweise als „Zero Trust“ bezeichnen. Trotz der großartigen Zero Trust-Forschung, die von Forrester's Dr. Chase Cunningham und Gartner's Neil MacDonald durchgeführt wurde, gab es bis zu diesem Buch keinen praktischen definitiven Leitfaden zu Zero Trust.

Glücklicherweise sind die Autoren Jason Garbis und Jerry Chapman hocherfahrene Technologen und Praktiker, die als anerkannte Experten in Zero Trust, Unternehmensnetzwerkbetrieb, Cybersicherheit und Geschäftsbetrieb gelten. Ich ermutige Sie, ihre Biografien zu lesen, da ihre Qualifikationen beeindruckend und unverfälscht sind. Um es mit militärischem Jargon zu sagen, sie haben „Das schon erlebt, das schon gemacht“.

In den folgenden Kapiteln liefern Jason und Jerry ein hervorragendes Buch, das eine unschätzbare Erklärung von Zero Trust präsentiert, die meiner Meinung nach als das endgültige Referenzwerk für Studenten und Praktiker überall verwendet werden sollte.

Die Organisation des Inhalts ist hervorragend. Diejenigen, die nicht mit dem Konzept des Zero Trust vertraut sind, und sogar diejenigen, die es sind, werden von den ersten vier Kapiteln profitieren, die einen strategischen Überblick über die Zero Trust-Reise bieten. Kap. 1 bietet eine aufschlussreiche Diskussion, die die Frage beantwortet: „Warum wird Zero Trust benötigt?“ Diejenigen, die gerade ihre Zero Trust-Reise beginnen, werden Kap. 2 als unschätzbar wertvoll empfinden,

da die Autoren eine ausgezeichnete Chronik darüber liefern, wie wir zur heutigen Zero Trust-Umgebung gekommen sind und klar definieren, was Zero Trust ist und was nicht. Diejenigen, die versuchen zu sehen, wie sie Zero Trust in ihre Betriebsarchitekturen integrieren können, werden den praktischen Rat und die lebendigen Beschreibungen zu schätzen wissen, die in Kap. 3 präsentiert werden. Viele Menschen, einschließlich mir selbst, ziehen es vor, dass andere „Flugtests" von Fähigkeiten durchführen, bevor sie bedeutende Investitionen tätigen oder größere strategische Änderungen vornehmen. Wir werden in Kap. 4 mit einer umfassenden Diskussion belohnt, wie Organisationen wie Google Zero Trust in ihren Betrieb integriert haben.

Der zweite Teil des Buches bietet einen hervorragenden Überblick über die wesentlichen Komponenten von Zero Trust, beginnend mit Kap. 5's außergewöhnlicher Diskussion über Identität. Ich behaupte, dass Identität die Kernkomponente jeder erfolgreichen Zero Trust-Implementierung ist und war erfreut zu sehen, dass Jason und Jerry diesen Abschnitt des Buches mit diesem Kapitel beginnen. Die nächsten drei Kapitel bieten eine wichtige Diskussion über die Auswirkungen von Zero Trust auf die Netzwerkinfrastruktur, die Netzwerkzugangskontrolle und die Systeme zur Erkennung und Abwehr von Eindringlingen. Wenn Sie diese drei Kapitel provokativ finden, wird Kap. 9's Diskussion über virtuelle private Netzwerke in einer Zero Trust-Welt wahrscheinlich die Art und Weise ändern, wie Sie die heutige Umgebung und die anhaltende Bewegung zu einer Arbeit-von-überall-Zukunft sehen.

Die Diskussion in Kap. 10 über Next-Generation Firewalls (NGFWs) ist ebenso provokativ, da die Autoren die Geschichte und Entwicklung der betreffenden Fähigkeiten diskutieren und ihre Zukunft in einer Welt des Zero Trust prognostizieren. Die Diskussion in Kap. 11 über Security Information and Event Management (SIEM) und Security Orchestration, Automation, and Response (SOAR) in einem Zero Trust Modell ist ein Muss für diejenigen, die sich auf die Identifizierung, das Management und die Kontrolle von Risiken konzentrieren. Diejenigen, die die Diskussion in Kap. 5 über Identität außergewöhnlich finden, werden von der Diskussion in Kap. 12 über Privileged Access Management nicht enttäuscht sein. Organisationen, die bestrebt sind, ihr Risiko von Insider-Bedrohungen zu reduzieren, sollten dem ebenfalls besondere Aufmerksamkeit schenken!

Die nächsten vier Kapitel bieten praktische Analysen und Anleitungen zu aktuellen technischen Problemen, mit denen viele Organisationen heute konfrontiert sind. Die Diskussion in Kap. 13 über Datenschutz ist außergewöhnlich und etwas, dem meine Studenten am Heinz College der Carnegie Mellon University besondere Aufmerksamkeit schenken sollten (das ist ein nicht allzu subtiler Hinweis vom Professor!). Die Diskussion in Kap. 14 über Cloud-Ressourcen bietet unkomplizierte praktische Ratschläge, wie man Zero Trust richtig anwendet, wenn man in Cloud-basierten Umgebungen arbeitet. Da viele Organisationen Technologien wie Software as a Service, Secure Web Gateways und Cloud Access Security Broker einsetzen, bietet Kap. 15 eine hervorragende Diskussion darüber, wie diese Technologien in Ihre Zero Trust-Strategie integriert werden können und gibt praktische Ratschläge, wie man es „richtig macht". Schließlich war ich begeistert, die Einbeziehung von Jason und Jerry's Diskussion in Kap. 16 über Internet of Things-Geräte und „Dinge" zu sehen. Zu viele Cybersicherheitspersonal sind auf Informationstechnologiegeräte fixiert und ignorieren die Risiken, die mit organisationaler Betriebstechnologie, industriellen Steuerungssystemen und „Internet of Things"-Geräten verbunden sind. Unabhängig von Ihrer organisatorischen Rolle, bitte beachten Sie dieses Kapitel und erkennen Sie die Bedeutung der Anwendung von Zero Trust beim Schutz dieser wichtigen Systeme.

Den Abschluss des Buches bilden drei Kapitel, die für jede Organisation, die sich dazu verpflichtet hat, Zero Trust in ihren Organisationen richtig umzusetzen, von entscheidender Bedeutung sind. Kap. 17 bietet eine wesentliche Diskussion darüber, wie man ein aussagekräftiges Zero Trust-Politikmodell erstellt und implementiert. Kap. 18 bietet unschätzbare Diskussionen über die wahrscheinlichsten Anwendungsfälle, die Ihre Organisation behandeln wird, wenn Sie Ihre Zero Trust-Implementierung ausrollen. Kap. 19 ist ein willkommener Begleiter zum vorherigen Kapitel, da es diskutiert, wie Organisationen Zero Trust angehen sollten, um die größte Wahrscheinlichkeit für Erfolg zu haben. Diejenigen, die an das Mantra „klein anfangen, groß denken und schnell skalieren" glauben, werden von Jasons und Jerrys praktischen Ratschlägen nicht enttäuscht sein. Schließlich bietet Kap. 20 einen zufriedenstellenden Abschluss der Reise des Buches durch Zero Trust, mit der Erinnerung daran, dass Sicherheit dazu dient, Organisationen bei der Erreichung ihrer Ziele zu unterstützen.

Zero Trust ist nicht nur ein eingängiger Aphorismus, es liegt in unserer Reichweite und wartet darauf, überall implementiert zu werden. Dieses Buch wird Ihnen helfen, Ihre Zero Trust-Ziele mit Geschwindigkeit und Präzision zu erreichen. Staatsakteure und Cyberkriminelle haben bewiesen, dass das auf dem Perimeter basierende Sicherheitsmodell nicht mehr gültig ist. So auch bemerkenswerte Insider-Schurken wie Edward Snowden. Die Zeit, sich schnell und gezielt auf das Zero Trust-Sicherheitsmodell zu bewegen, ist jetzt. Dank der aufschlussreichen Arbeit von Jason Garbis und Jerry Chapman haben wir nun einen praktischen Leitfaden, wie wir unsere Zero Trust-Ziele erreichen können.

Generäle seit Sun Tzu und Alexander dem Großen implementierten das perimeterbasierte Sicherheitsmodell, um ihre Vermögenswerte zu verteidigen. Sie hatten nicht das Internet, mobile Geräte, Cloud-Computing und andere moderne Technologien. Das Jericho Forum hat es richtig gemacht; der Perimeter ist tot. Jetzt ist es an der Zeit, Zero Trust überall zu umarmen und zu implementieren. Unsere nationale Sicherheit und nationaler Wohlstand verdienen nichts weniger.

—Gregory J. Touhill, CISSP, CISM,
Brigadegeneral, USAF (im Ruhestand)

TEIL I

Zero Trust Security

Zero Trust ist eine Sicherheitsphilosophie und ein Satz von Prinzipien, die zusammen eine bedeutende Veränderung darstellen, wie Unternehmens-IT und Sicherheit angegangen werden sollten. Die Ergebnisse können enorm vorteilhaft für Sicherheitsteams und für Unternehmen sein, aber Zero Trust ist breit gefächert und kann überwältigend sein. Im Teil I dieses Buches werden wir Ihnen eine historische und grundlegende Einführung in Zero Trust geben, erklären, was es ist (und was es nicht ist), und Zero Trust-Architekturen in Theorie und Praxis darstellen. Dies wird Ihnen helfen, Zero Trust Stück für Stück zu verstehen und darüber nachzudenken, wie es angewendet werden kann, um die Sicherheit, Widerstandsfähigkeit und Effizienz Ihrer Organisation zu verbessern.

KAPITEL 1

Einführung

Unternehmenssicherheit ist schwierig. Dies liegt an der Komplexität von IT- und Anwendungsinfrastrukturen, der Breite und Geschwindigkeit des Benutzerzugriffs und natürlich der inhärent adversen Natur der Informationssicherheit. Es liegt auch an der allzu offenen Natur der meisten Unternehmensnetzwerke – indem sie das Prinzip der geringsten Privilegien sowohl auf Netzwerk- als auch auf Anwendungsebene nicht durchsetzen, machen sich Organisationen unglaublich anfällig für Angriffe. Dies gilt sowohl für interne Netzwerke als auch für öffentliche, dem Internet zugewandte Remote-Zugangsdienste wie Virtual Private Networks (VPNs). Die letzteren sind jedem Gegner im Internet ausgesetzt. Angesichts der heutigen Bedrohungslandschaft würden Sie niemals ein System auf diese Weise entwerfen. Und doch perpetuieren traditionelle Sicherheits- und Netzwerksysteme, die nach wie vor weit verbreitet sind, dieses Modell.

Zero Trust-Sicherheit, das Thema dieses Buches, ändert dies und bringt einen modernen Ansatz zur Sicherheit, der das Prinzip der geringsten Privilegien für Netzwerke und Anwendungen durchsetzt. Nicht autorisierte Benutzer und Systeme haben überhaupt keinen Zugriff auf Unternehmensressourcen, und autorisierte Benutzer haben nur den minimal notwendigen Zugriff. Das Ergebnis ist, dass Unternehmen sicherer, geschützter und widerstandsfähiger sind. Zero Trust bringt auch Verbesserungen in Effizienz und Effektivität durch die automatisierte Durchsetzung dynamischer und identitätszentrierter Zugriffsrichtlinien.

Bitte beachten Sie, dass das „Zero“ in Zero Trust ein wenig irreführend ist – es geht nicht buchstäblich um „null“ Vertrauen, sondern um null *inhärentes* oder *implizites*Vertrauen. Zero Trust geht darum, sorgfältig eine Vertrauensbasis aufzubauen und dieses Vertrauen zu erweitern, um letztendlich ein angemessenes Zugriffsniveau zur richtigen Zeit zu ermöglichen. Es hätte vielleicht „verdientes Vertrauen“ oder „adaptives Vertrauen“ oder „null implizites Vertrauen“ genannt werden können, und diese hätten der Bewegung besser entsprochen, aber „Zero Trust“ hat mehr Pep, und es hat sich durchgesetzt. Bitte nehmen Sie das „Zero“ nicht wörtlich!

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_1

Zero Trust ist ein wichtiger und sehr sichtbarer Trend in der Informationssicherheitsbranche, und obwohl es zu einem Marketing-Buzzword geworden ist, glauben wir, dass dahinter echte Substanz und Wert stecken. Im Kern ist Zero Trust eine Philosophie und ein Ansatz sowie eine Reihe von Leitprinzipien. Das bedeutet, dass es so viele Möglichkeiten gibt, Zero Trust zu interpretieren, wie es Unternehmen gibt. Es gibt jedoch grundlegende und universelle Prinzipien, denen jede Zero Trust-Architektur folgen wird. In diesem Buch werden wir Richtlinien und Empfehlungen für Zero Trust auf der Grundlage unserer Erfahrungen mit Unternehmen verschiedener Größen und Reifegrade auf ihrem Weg zu Zero Trust geben. Denken Sie daran, wir verwenden das Wort *Reise* absichtlich; dies soll unterstreichen, dass es sich nicht um ein einmaliges Projekt handelt, sondern um eine fortlaufende und sich entwickelnde Initiative. Und deshalb haben wir dieses Buch geschrieben – um unsere Gedanken und Empfehlungen darüber zu teilen, wie Sie Zero Trust in Ihrer Umgebung am besten angehen können und um Sie auf Ihrer Reise zu begleiten.

Wir glauben grundsätzlich, dass Zero Trust ein besserer und effektiverer Weg ist, um Unternehmenssicherheit zu erreichen. In gewisser Weise wurde Zero Trust eng mit Netzwerksicherheit in Verbindung gebracht, und obwohl Netzwerke ein Kernbestandteil von Zero Trust sind, werden wir auch die volle Breite der Zero Trust-Sicherheit erforschen, die Grenzen in Anwendungen, Daten, Identitäten, Operationen und Richtlinien überschreitet.

Als Sicherheitsleiter haben Sie die Verantwortung, Ihre Organisation dazu zu drängen, zu ziehen und zu stoßen, diesen neuen Ansatz zu übernehmen, der die Widerstandsfähigkeit Ihrer Organisation verbessern und Ihnen auch helfen wird, professionell zu wachsen. Dieses Buch – Ihr Leitfaden – ist in drei Teile gegliedert. Teil I bietet eine Einführung in die Zero Trust-Prinzipien und legt den Rahmen und das Vokabular fest, die wir verwenden werden, um Zero Trust zu definieren und IT- und Sicherheitsinfrastruktur auszurichten. Dies sind die Grundlagen dessen, was wir für notwendig halten, um die vollständige Zero Trust-Geschichte zu erzählen.

Teil II ist ein tiefer Einblick in IT- und Sicherheitstechnologien und ihre Beziehung zu Zero Trust. Hier beginnen Sie zu sehen, wie Ihre Organisation Zero Trust nutzen kann und wo Sie Ihre aktuelle IT- und Sicherheitsinfrastruktur in eine modernere Architektur integrieren können. Da Zero Trust einen identitätszentrierten Ansatz zur Sicherheit verfolgt, werden wir untersuchen, wie verschiedene Technologien beginnen können, von Identitätskontexten zu profitieren und effektiver zu werden.

Teil III bringt alles zusammen und baut auf den ersten beiden Teilen des Buches auf, die eine konzeptionelle Grundlage und eine tiefe Technologiediskussion lieferten. Dieser Teil untersucht, wie ein Zero Trust-Richtlinienmodell aussehen sollte, untersucht spezifische Zero Trust-Szenarien (Anwendungsfälle) und diskutiert schließlich einen strategischen und taktischen Ansatz, um Zero Trust erfolgreich zu machen.

Es ist auch wichtig zu beachten, dass wir uns bewusst dafür entschieden haben, Anbieter oder Anbieterprodukte im Rahmen dieses Buches nicht zu bewerten. Unsere Branche bewegt sich zu schnell – das Innovationstempo ist hoch – und solche Bewertungen hätten eine sehr kurze Haltbarkeit. Stattdessen konzentrieren wir uns auf die Erforschung architektonischer Prinzipien, aus denen Sie Anforderungen ableiten können und die Sie zur Bewertung von Anbietern, Plattformen, Lösungsanbietern und Ansätzen verwenden können.

Wenn Sie das Ende dieses Buches erreichen, sollte klar sein, dass es keinen einzig richtigen Ansatz für Zero Trust gibt. Sicherheitsleiter müssen bestehende Infrastrukturen, Prioritäten, Mitarbeiterfähigkeiten, Budgets und Zeitpläne berücksichtigen, während sie ihre Zero Trust-Initiative entwerfen. Dies mag Zero Trust kompliziert erscheinen lassen, aber seine Breite des Anwendungsbereichs hilft tatsächlich, Unternehmenssicherheit und Architektur zu vereinfachen. Als Overlay-Sicherheits- und Zugriffsmodell normalisiert es Dinge und gibt Ihnen eine zentralisierte Möglichkeit, Zugriffsrichtlinien in einer verteilten und heterogenen Infrastruktur zu definieren und durchzusetzen.

Letztendlich ist das Ziel dieses Buches, Ihnen ein solides Verständnis dessen zu vermitteln, was Zero Trust ist, und das Wissen, um die einzigartige Reise Ihrer Organisation zu Zero Trust erfolgreich zu steuern. Wenn Sie dies erreichen, waren unsere Bemühungen erfolgreich. Lassen Sie uns unsere Reise beginnen.

KAPITEL 2

Was ist ZeroTrust?

In diesem Kapitel werden wir Zero Trust als Konzept, Philosophie und Rahmenwerk einführen. Neben einem kurzen Überblick über die Geschichte und Entwicklung von Zero Trust werden wir auch einige Leitprinzipien vorstellen. Wir glauben, dass es *kern* und *erweiterte* Prinzipien gibt, die für jede Zero Trust-Initiative gemeinsam sind und die wichtig zu verstehen sind, wenn Sie Ihre Reise beginnen. Unser Ziel für dieses Kapitel ist es, Ihnen eine Arbeitsdefinition von Zero Trust auf der Grundlage dieser Prinzipien zu geben und einen Satz grundlegender Plattformanforderungen bereitzustellen.

Geschichte und Entwicklung

Traditionell wurden Sicherheitsgrenzen am Rand des Unternehmensnetzwerks in einem klassischen „Burgmauer und Graben"-Ansatz platziert. Mit der Entwicklung der Technologie wurden jedoch Remote-Mitarbeiter und Remote-Workloads immer häufiger. Sicherheitsgrenzen folgten notwendigerweise und erweiterten sich von nur dem Unternehmensperimeter auf die Geräte und Netzwerke, mit denen der Remote-Benutzer verbunden war, und die Ressourcen, mit denen sie sich verbanden. Dies zwang Sicherheits- und Netzwerkteams, diese Geschäftsanforderungen zu berücksichtigen und die Modelle anzupassen, nach denen Organisationen Sicherheit und Zugang anwendeten, mit gemischtem Erfolg.[1]

Im Jahr 2010 führte Forrester-Analyst John Kindervag den Begriff "Zero Trust" in dem einflussreichen Weißbuch "No More Chewy Centers: Introducing The Zero Trust

[1]Wir versuchen, mit dieser Aussage diplomatisch zu sein. Es ist eine unbestreitbare Tatsache, dass die Sicherheit von Unternehmensnetzwerken und Daten als Branche es nicht geschafft hat, unsere Organisationen effektiv vor Datenverlust und Systemverletzungen zu schützen. Zugegeben, wir stehen ausgeklügelten und motivierten Gegnern gegenüber, aber wir glauben, dass dieses weit verbreitete Versagen hauptsächlich auf die Mängel traditioneller Infosec-Tools und -Ansätze zurückzuführen ist und dass Zero Trust weitaus effektiver sein wird.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_2

Model Of Information Security"[2] ein. Dieses Papier fasste Ideen zusammen, die in der Branche seit einigen Jahren diskutiert wurden, insbesondere vom Jericho Forum gefördert. Das Forrester-Dokument beschrieb den Wandel weg von einem harten Perimeter und hin zu einem Ansatz, der erforderte, Elemente innerhalb eines Netzwerks zu inspizieren und zu verstehen, bevor sie ein Vertrauens- und Zugangsniveau verdienen konnten. Im Laufe der Zeit entwickelte Forrester dieses Konzept zu dem, was heute als *Zero Trust eXtended* (ZTX) Framework bekannt ist, das Daten, Workloads und Identität als Kernkomponenten von Zero Trust umfasst.

Zur gleichen Zeit begann Google ihre interne BeyondCorp-Initiative, die eine Version von Zero Trust implementierte und grundlegende Zero Trust-Elemente einführte, die effektiv ihre Unternehmensnetzwerkgrenze entfernten. Seit 2014 beeinflusste Google die Branche stark mit einer Reihe von Artikeln, die ihre bahnbrechende interne Implementierung dokumentierten. Ebenfalls im Jahr 2014 stellte die Cloud Security Alliance die Software Defined Perimeter (SDP) Architektur vor, die eine konkrete Spezifikation für ein Sicherheitssystem lieferte, das Zero Trust-Prinzipien unterstützt.[3] Wir werden sowohl BeyondCorp als auch SDP später im Kap. 4 durch die Linse von Zero Trust betrachten.

Im Jahr 2017 überarbeitete das Branchenanalystenunternehmen Gartner ihr Continuous Adaptive Risk and Trust Assessment (CARTA) Konzept, das viele Prinzipien mit Zero Trust gemeinsam hat. CARTA bietet nicht nur Identitäts- und Datenelemente, sondern beinhaltet auch Risiko- und Haltungselemente, die mit Identität und Geräten verbunden sind, die auf die Umgebung zugreifen.

Die branchenweite Betonung von Zero Trust setzte sich fort, als das US National Institute of Standards and Technology (NIST) eine Zero Trust Architecture-Publikation[4] und ein zugehöriges US National Cybersecurity Center of Excellence-Projekt im Jahr 2020 veröffentlichte.[5]

Zero Trust entwickelt sich weiter, da Anbieter und Normungsorganisationen Spezifikationen und Implementierungen von Zero Trust überprüfen und verfeinern und

[2]Forrester, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security", September 2010.

[3]Siehe den CSA's Architecture Guide für SDP, https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/.

[4]NIST Special Publication 800.207—Zero Trust Architecture, https://csrc.nist.gov/publications/detail/sp/800-207/final, August 2020.

[5]https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture.

es als grundlegende Veränderung im Ansatz zur Informationssicherheit anerkennen. Letztendlich hat die Branche zugestimmt, dass diese Änderungen und Verfeinerungen notwendig sind, um zu verhindern, dass böswillige Akteure auf private Ressourcen innerhalb organisatorischer Grenzen zugreifen, Daten exfiltrieren und den Betrieb stören.

Wir, die Autoren dieses Buches, arbeiten in der Informationssicherheitsbranche und verbringen beide viel Zeit damit, mit Sicherheitsfachleuten über Zero Trust zu sprechen. Eine häufig gestellte Frage, die wir hören, ist: „Was ist neu an Zero Trust – wie unterscheidet es sich von dem, was bereits getan wurde?“ Es ist definitiv wahr, dass einige Elemente von Zero Trust, wie *Zugriff mit minimalen Privilegien* und *rollenbasierte Zugriffskontrolle* Prinzipien sind, die in der aktuellen Netzwerk- und Sicherheitsinfrastruktur häufig implementiert werden (und in Zero Trust-Umgebungen genutzt werden müssen), aber allein vervollständigen sie das Bild nicht.

Grundlegende Sicherheitselemente, die vor Zero Trust verwendet wurden, erreichten oft nur eine grobe Trennung von Benutzern, Netzwerken und Anwendungen. Zum Beispiel sind in den meisten Organisationen Entwicklungsumgebungen von Produktionsumgebungen getrennt. Zero Trust verstärkt dies jedoch, indem es effektiv verlangt, dass alle Identitäten und Ressourcen voneinander getrennt werden. Zero Trust ermöglicht feinkörnige, identitäts- und kontextsensitive Zugriffskontrollen, die von einer automatisierten Plattform gesteuert werden. Obwohl Zero Trust als ein eng fokussierter Ansatz begann, Netzwerkidentitäten nicht zu vertrauen, bis sie authentifiziert und autorisiert waren, hat es sich zu Recht zu einem viel breiteren Satz von Sicherheitsfähigkeiten in der Umgebung einer Organisation entwickelt.

Lassen Sie uns kurz die Zero Trust-Modelle von Forrester und Gartner betrachten, bevor wir das, was wir für die Schlüsselprinzipien von Zero Trust halten, vorstellen.

Forresters Zero Trust eXtended (ZTX) Modell

Forrester veröffentlichte ihr anfängliches Zero Trust-Modell im Jahr 2010, und in den folgenden Jahren wurde es überarbeitet und erneut als *Zero Trust eXtended* (ZTX) veröffentlicht. ZTX bietet reichhaltigeren Inhalt und ein ausgewogenes Modell, das Daten in den Mittelpunkt stellt, wie in Abb. 2-1 gezeigt. Dies spiegelt Forresters Überzeugung wider, dass die Datenexplosion sowohl in On-Prem- als auch in Cloud-Umgebungen im Zentrum dessen steht, was geschützt werden muss. Die umgebenden