Digital Security
Progress. Protected.

ZERO TRUST VERSTEHEN, SECURITY STÄRKEN

INHALTSANGABE

EINLEITUNG

So mancher Verantwortlicher für IT-Sicherheit agiert wie ein Manager eines professionellen Fußballclubs. Da wird die beste Elf zusammengekauft, von einem renommierten Trainer betreut und dann aufs Feld geschickt. Und tatsächlich: Es funktioniert, ein Sieg reiht sich an den nächsten. Allerdings nur bis zu dem Tag, wo der Gegner plötzlich gewinnt. Hat er das System geknackt, Schwächen gefunden oder einfach nur Glück gehabt? Was auch immer der Grund war, die finanziellen Schäden können immens sein, wenn ein wichtiges Match verloren geht.

Dieselbe Frage stellt sich auch in der IT-Security – die Analogie ist verblüffend. So mancher Administrator setzt auf die besten technischen Sicherheitslösungen und investiert dafür viel Geld. Und doch machen ihm Cyberkriminelle irgendwann einen Strich durch die Rechnung. Dabei spielt es keine Rolle, ob er für den Deutschen Bundestag, Kliniken, Landkreisverwaltungen, Möbelhausketten oder Elektromärkte arbeitet. Hacker attackieren alles und erfolgreich, was nicht gut genug abgesichert wurde.

Das eigentlich Unglaubliche ist: Oftmals sind gar keine Meisterleistungen der Kriminellen vonnöten. Wie konnten sie das Abwehrbollwerk umgehen, wenn doch die besten Spieler aufgeboten sind? Möglicherweise liegt es daran, dass man die Grundtugenden vernachlässigt, wenn die Stärken doch so ausgeprägt sind – im Fußball wie auch in der IT-Security. TikiTaka und Hackentricks erfreuen sicher alle, doch wenn die Kampfkraft und das Bewusstsein um die eigenen Schwächen fehlen, geht der Schuss nach hinten los.

Die Liste der vermeidbaren Fehler scheint nicht abzureißen. Microsoft Exchange-Lücken waren zum Beispiel lang genug bekannt und wurden wider besseres Wissen nicht gestopft. Phishing-Mails übertölpeln nach wie vor viele Anwender und gelten als das Sprungbrett für Ransomware-Angriffe. Und wenn kostenfreie Produkte wie das Remote Dektop Protocol (RDP) von Microsoft statt kostenpflichtiger Lösungen wie Virtual Private Network (VPN) eingesetzt werden, dann darf man sich nicht wundern, wenn Cyberkriminelle auf der Siegeswelle reiten.

Dies lässt nur einen Schluss zu: Mit herkömmlichen Mitteln und Plänen der eigenen Stärken wird man nicht Herr der Lage. Gerade der Kampf gegen Hacker zeigt deutlich, dass das bloße Aneinanderreihen von Sicherheitsmaßnahmen

nicht mehr ausreicht. Eine strategische Lösung muss her, die auch Antworten auf das Risiko durch „weiche“ Gefahrenfaktoren – vom einzelnen Mitarbeiter bis zur ungepatchten Schwachstelle - miteinbeziehen.

Und so verwundert es manchen, dass eine Idee aus den Anfängen des Internets seine Renaissance feiert: Zero Trust. Der nicht ganz „taufrische“ Ansatz für mehr IT-Sicherheit rückt für viele Organisationen wieder in den Fokus. Doch welche Idee steckt hinter Zero Trust oder ist es wieder nur ein sogenanntes „Buzzword“, das temporär durch die IT-Szene wabert? Warum ist Zero Trust wieder so aktuell, obwohl es die letzten Jahre mehr oder weniger in der Versenkung verschwand? Genau diesen Fragen gehen wir in diesem Paper nach und zeigen anhand des ESET Reifegradmodells, wie sich das Grundprinzip in der Praxis umsetzen lässt.

Was ist Zero Trust?

DIE ZEITLICHE ENTWICKLUNG VON ZERO TRUST

Im Jahr 2010 prägte John Kindervag, ein Analyst von Forrester Research, den Begriff „Zero Trust". Seine Veröffentlichung „No More Chewy Centers: Vorstellung des Zero Trust Informationssicherheits-Modells" sorgte für großes Aufsehen. Zwei weitere Berichte folgten, in denen er en detail das Konzept und die Architektur von Zero Trust beschrieb. Die von ihm vorgestellte primäre Richtlinie wird noch heute als Grundidee zitiert: „Gemäß Zero Trust ist der gesamte Netzwerkverkehr nicht vertrauenswürdig. Daher müssen Sicherheitsexperten alle Ressourcen überprüfen und sichern, die Zugriffskontrolle einschränken und strikt durchsetzen sowie den gesamten Netzwerkverkehr überprüfen und protokollieren."

Streng genommen ist Kindervag aber nicht der Urvater dieser Idee zur IT-Sicherheit. Bereits 1994 beschäftigte sich Stephan Marsh in seiner Doktorarbeit an der University of Stirling mit dem Problem der Computersicherheit: „Formalising Trust as a Computational Concept, Dissertation". Er führte zum ersten Mal den Begriff des Vertrauens („Trust") in die IT-Security ein. Allerdings war Marsh seiner Zeit noch weit voraus.

2004 gründeten die Chief Information Security Officer (CISO) verschiedener Unternehmen das sogenannte Jericho-Forum. Die Organisation ging der Frage nach, wie sich die IT-Sicherheit in Architekturen aufrechterhalten lässt, wenn sich Netzwerkgrenzen auflösen und klassische Perimeter-orientierte Sicherheitskonzepte nicht mehr den gewünschten Erfolg bringen („De-Perimeterisierung"). Deswegen war man der Ansicht, dass Firewall, Virenschutz & Co. in offenen IT-Systemen ungeeignet sind. In diesem Umfeld spielen Verschlüsselung, Authentifizierung, sichere Protokolle und selbstkontrollierende Systeme eine viel wichtigere Rolle. In den sogenannten Jericho Forums-Geboten definierten die Mitglieder Bereiche und Prinzipien, die bei der Planung einer *de-perimeterisierten* Zukunft zu beachten sind. Das Konzept von Zero Trust nimmt Form an.

2009 setzte Google sein selbst entwickeltes Zero Trust-Modell BeyondCorp in die Praxis um. In diesem Modell werden die Zugriffskontrollen von der Netzwerkumgebung auf individuelle Nutzer verschoben. Mit BeyondCorp können Mitarbeiter von praktisch jedem Ort aus ohne herkömmliches VPN sicher arbeiten. Eine nutzer- und gerätebasierte Authentifizierung und Autorisierung ermöglicht

den Zugang zur Kerninfrastruktur und zu Unternehmensressourcen von Google.

2017 entwickelten die Marktforscher von Gartner ihren CARTA-Ansatz. „Continuous Adaptive Risk and Trust Assessment" führt das ursprüngliche Prinzip von Zero Trust weiter. Nach CARTA gilt es, Nutzer, Geräte und Apps nicht nur bei jeder Anmeldung zu prüfen, sondern deren Vertrauensstatus fortlaufend während der Session zu hinterfragen. Wird eine Veränderung festgestellt, die ein Risiko bedeuten könnte, kann der gewährte Zugang zu einem Service eingeschränkt oder ganz unterbrochen werden.

Im Februar 2020 – also noch vor der Corona-Pandemie – nahm der Zero Trust-Zug endlich Fahrt auf. Einer Umfrage von Cybersecurity Insiders und Pulse Secure zufolge gaben 72 Prozent der mehr als 400 befragten IT-Sicherheitsentscheidern an, Zero Trust im Laufe des Jahres in ihre Sicherheitsstrategie aufzunehmen oder zu implementieren.

Im Mai 2021 erhielt das Zero Trust-Konzept seinen Ritterschlag. US-Präsident Biden warf mit seiner „Executive Order on Improving the Nation's Cybersecurity" Hackern den Fehdehandschuh hin. Er räumte dabei den desolaten Zustand des US-Bundesmodells der Cybersicherheit ein und ordnete die Implementierung einer Zero Trust-Architektur an.

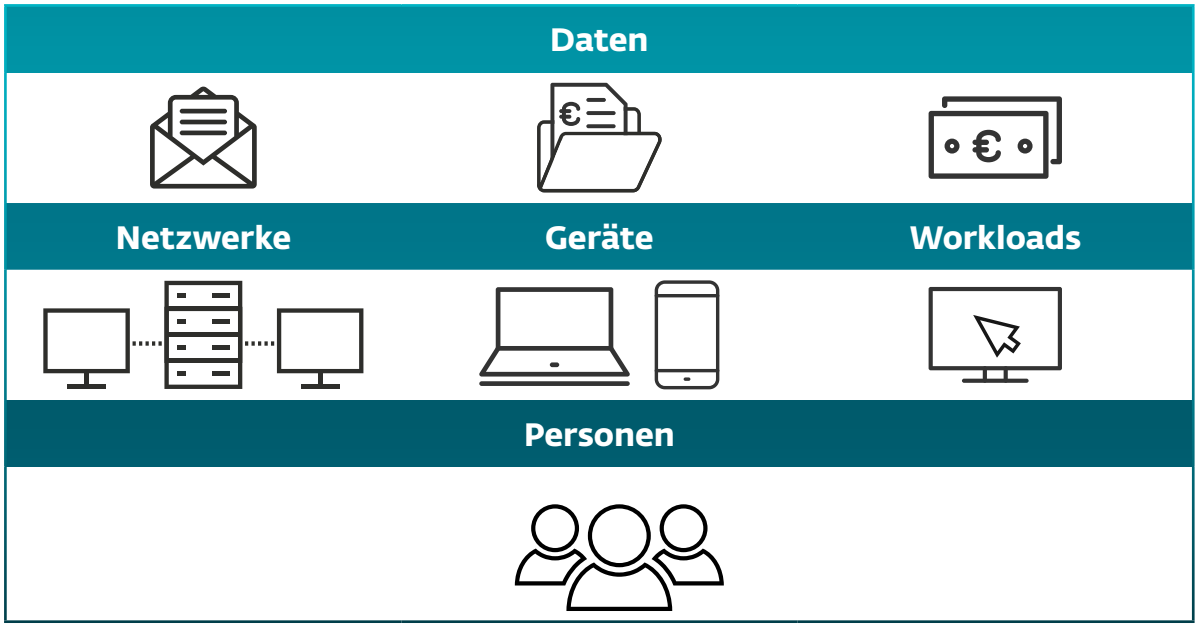
Sicherheit existiert, um Vertrauen zu ermöglichen. Vertrauen ist das Ziel, und Sicherheit ist die Art und Weise, wie wir es ermöglichen.

Bruce Schneier, Experte für Kryptographie und Computersicherheit

WAS STECKT HINTER DEM BEGRIFF ZERO TRUST?

Hinter Zero Trust steht die Idee einer konzeptionellen Leitlinie, die auf Vorsicht und Skepsis beruht. Es handelt sich also nicht um eine Blaupause für ein IT-Sicherheitssystem oder eine technisch ausgefeilte Securitylösung. Laut Forrester beruht die Prämisse von Zero Trust darauf, keiner Entität zu vertrauen, weder intern noch extern. Mit anderen Worten: „Vertraue nie, überprüfe immer". Experten beschreiben Zero Trust als ein perimeterloses Modell. Dieses muss ständig aktualisiert werden, um Daten, Software und andere Anwendungen unabhängig von Nutzern, Standort oder Geräteart zu schützen.

Das Zero Trust-Modell baut die Sicherheit um jede der wichtigsten Ressourcen und Entitäten einer Organisation herum auf: Daten, Netzwerke, Geräte, Workloads und Personen.



- **Daten:** Organisationen klassifizieren ihre Daten und sorgen mit Verschlüsselung dafür, dass sie sicher gespeichert und übertragen werden. Auch die Überwachung der Dateiintegrität und die Verhinderung von Datenverlust tragen zur Datensicherung bei.

- **Netzwerke:** Mikrosegmentierung ist hier wichtig. Über Netzwerkgeräte wie Router und Switches in Kombination mit Access Control Lists (ACLs) kann eingeschränkt werden, wer und was mit verschiedenen Teilen des Netzwerks kommunizieren kann. Wichtig ist auch der Umgang mit Schwachstellen.

- **Geräte:** Mittels Asset Management verstehen Netzwerkbetreiber besser, welche Geräte sich im Einsatz befinden. Moderne Security-Lösungen von Malware-Schutz über hostbasierte Firewalls bis Endpoint Detection and Response schützen diese Assets und verhindern die Verbreitung von Schadcode.

- **Workloads:** Die meisten Cloud-Anbieter bauen hier Kontrollen ein. Organisationen sollten diese verwenden, um den Zugriff auf verschiedene Workloads zu reduzieren.

- **Personen:** Rollenbasierte Zugriffskontrollen, Multi-Faktor-Authentifizierung und Kontentrennung sorgen dafür, dass nur Berechtigte die ihnen zugewiesenen Aufgaben erledigen dürfen.

Schließlich geht es um das Management und die Automatisierung der Sicherheitstools und die Nutzung von Datenanalysefunktionen. Das verschafft Security-Teams das nötige Situationsbewusstsein, um ihre Arbeit effektiv zu erledigen.

ERHOFFTE VORTEILE VON ZERO TRUST

Forrester nennt vor allem vier unterschiedliche Hauptvorteile, die Zero Trust liefert:

- Umfassender und fortwährender Schutz gegen Bedrohungen aller Art. Dazu zählen vor allem Advanced Persistent Threats und aktuell auch Ransomware.

- Generell verbesserte IT-Sicherheit sowohl im eigenen Netzwerk als auch auf externen Geräten von Remote Workern.

- Zuverlässiger Schutz von Daten und Anwendungen im eigenen Netzwerk und in der Cloud.

- Reduzierung von Sicherheitslücken durch permanente Kontrolle.

ZERO TRUST VS. PERIMETER-MODELL

Das Zero Trust-Modell steht im Gegensatz zum traditionellen, perimeterbasierten Sicherheitsmodell, das auf der Prämisse „Vertrauen, aber überprüfen" aufbaut. Schon frühzeitig erkannten die Experten des Analystenhauses Forrester, dass diese Vorgehensweise in absehbarer Zeit an seine Grenzen stoßen wird. Ihnen war klar, dass es nicht mehr ausreicht, alle Sicherheitsressourcen um die eigenen Systeme und Netzwerke herum zu platzieren und dann allem zu vertrauen, was sich darin befindet.

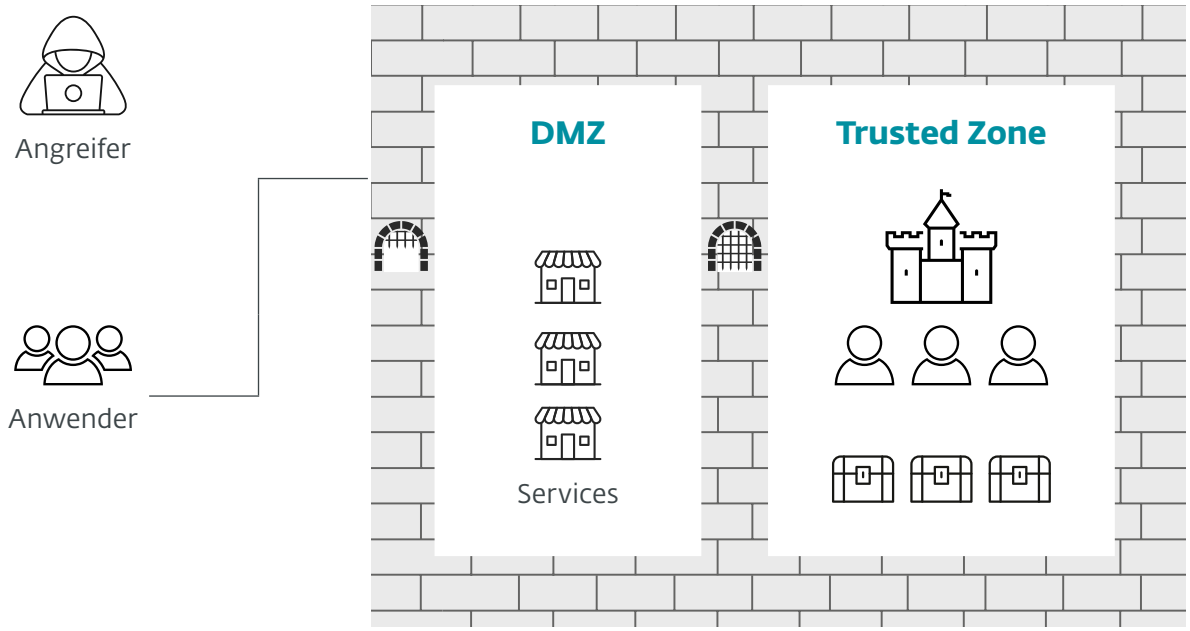
Stattdessen setzt Zero Trust auf „Niemals vertrauen, immer überprüfen", um die Auswirkungen von Sicherheitsverletzungen zu reduzieren. In der Praxis gibt es drei grundlegende Prinzipien:

1. **Alle Netzwerke sollten als nicht vertrauenswürdig behandelt werden**
   Dies sollte Heimnetzwerke, öffentliche WLAN-Netzwerke (z. B. in Flughäfen und Cafés) und sogar lokale Unternehmensnetzwerke umfassen. Bedrohungsakteure sind einfach zu entschlossen und fähig, als dass wir davon ausgehen könnten, dass es noch sichere Räume gibt.

2. **Prinzip der geringsten Berechtigungen**
   Wenn alle Netzwerke als nicht vertrauenswürdig angesehen werden, müssen Sie dies auch für die Benutzer annehmen. Schließlich können Sie nicht garantieren, dass ein Konto nicht gehackt wurde oder dass ein Benutzer kein böswilliger Insider ist. Das bedeutet, dass Mitarbeiter gerade genug Berechtigungen bekommen sollten, um ihre Arbeit zu erledigen. Anschließend sollten die Zugriffsrechte regelmäßig überprüft und alle Rechte, die nicht mehr angemessen sind, regelmäßig entfernt werden.

3. **Sicherheitsvorfälle berücksichtigen**
   Jeden Tag stehen neue Cyberangriffe in den Medien. Deswegen sollten Unternehmen eine Kultur und Praxis der Wachsamkeit pflegen und ihre Abwehrkräfte durch eine Zero Trust-Mentalität weiter verbessern. Sicherheitsverstöße sind letzten Endes unvermeidlich – es geht vielmehr darum, ihre Auswirkungen zu reduzieren.

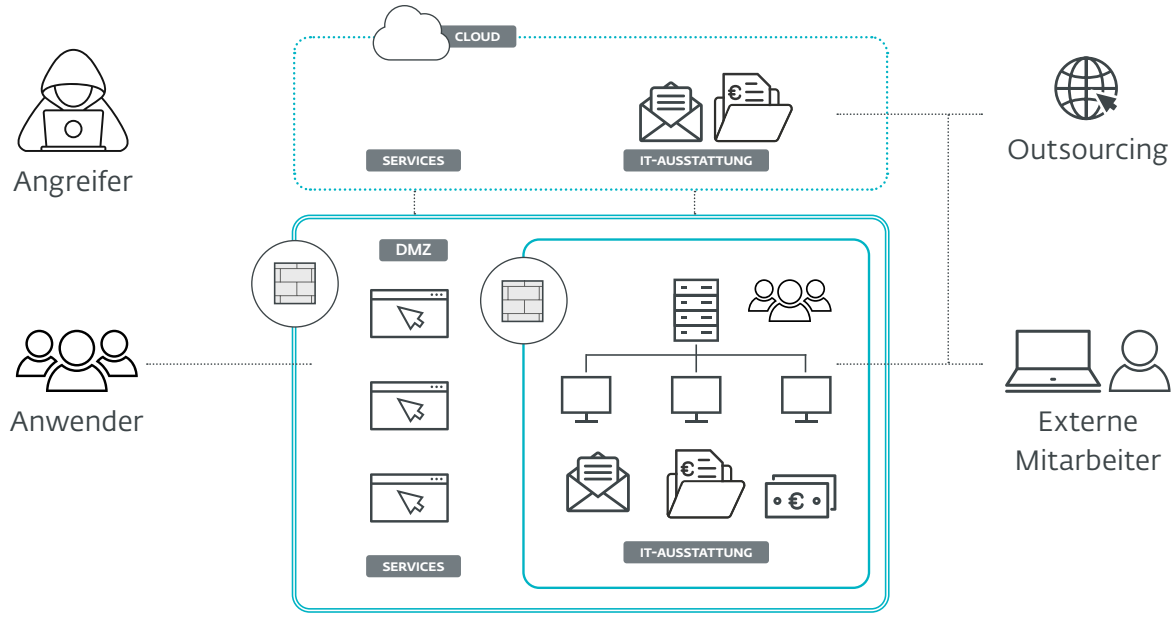
Als das Zero Trust-Modell im Jahr 2010 vorgestellt wurde, war es noch sehr netzwerkzentriert. Kein Wunder, denn zu dieser Zeit war der externe Zugriff auf das eigene Netzwerk stark limitiert. Nur wenige Mitarbeiter befanden sich damals im Home-Office; Dienstleister und Geschäftspartner erhielten nur stark eingeschränkte Zugriffsrechte auf einen gesonderten Teilbereich des Netzwerks. Im Laufe der Jahre hat es sich zu einem kompletten Ökosystem entwickelt. Im Zentrum stehen die kritischen Daten oder Geschäftsprozesse, die geschützt werden müssen.



Das traditionelle IT-Sicherheitsmodell einer Organisation ähnelt dem Konzept einer mittelalterlichen Burg. Wer diese angreifen oder einnehmen möchte, muss diverse Hürden überwinden. Der Burggraben, die dicken Mauern, die Zugbrücke und der bewachte Innenhof sind mit technischen Maßnahmen der IT-Sicherheit vergleichbar. Die Soldaten innerhalb der Burg kann man mit der Aufmerksamkeit des IT-Teams oder der Mitarbeiter gleichsetzen. In einem solchen Aufbau ist es schwierig, von außerhalb des Netzwerks Zugriff auf die Ressourcen einer Organisation zu erhalten. Gleichzeitig gilt jeder, der sich innerhalb des Netzwerks befindet, standardmäßig als vertrauenswürdig. Das Problem bei diesem Ansatz ist jedoch, dass, sobald ein Angreifer Zugriff auf das Netzwerk erlangt hat und damit standardmäßig als vertrauenswürdig gilt, alle Ressourcen der Organisation für ihn zur Verfügung stehen.

Im Gegensatz dazu geht das Zero Trust-Modell davon aus, dass sich Angreifer sowohl innerhalb als auch außerhalb des Netzwerks befinden. Aus diesem Grund kann Benutzern und Geräten nicht wahllos und standardmäßig Vertrauen geschenkt werden.

Forrester hat noch weitere wichtige Ebenen hinzugefügt: Automatisierung und Orchestrierung sowie Transparenz und Analyse. Diese integrieren alle tiefergehenden Kontrollen, die zur Unterstützung von Zero Trust erforderlich sind.



In dieser neuen Form ist Zero Trust ein perfektes Modell, um die Risiken eines hybriden Arbeitsplatzes zu mindern. Diese kennzeichnen sich dadurch, dass sich die Sicherheitsbereiche stets verändern, verteilte Mitarbeiter ständig authentifiziert werden müssen und Netzwerke segmentiert werden, um die Ausbreitungsmöglichkeiten von Bedrohungen zu reduzieren. Im Verlauf der Corona-Pandemie wurde auch deutlich, dass VPNs in vielen Fällen nicht darauf ausgelegt waren, eine große Anzahl von Fernarbeitern mit einer zuverlässigen Anbindung an das Unternehmensnetzwerk zu versorgen – sowohl im Hinblick auf den eingehenden Datenverkehr als auch bei der ausgehenden Last bei Patch-Auslieferungen. Und sie sind zunehmend auch selbst ein Ziel, wenn sie ungepatcht bleiben und schlecht geschützt werden. Zero Trust ist auf längere Sicht die bessere Option.

Teil 2:

Vom Erfolgsmodell zum Ladenhüter und zurück

WARUM WAR ZERO TRUST LANGE ZEIT WENIG ERFOLGREICH?

Zero Trust ist ein idealistisches Modell mit viel höherer Multidimensionalität als das klassische Perimeter Defense Modell. Als es 2010 veröffentlich wurde, konnte eigentlich fast keine Organisation die Ziele jemals wirklich erreichen. Die Ansprüche überforderten schlichtweg viele IT-Teams durch ihre Komplexität. Aber auch fehlende technische und finanzielle Ressourcen oder dynamische Veränderungen - wie beispielsweise Skalierung der Organisation - taten ihr Übriges. Und so mancher IT-Verantwortliche scheute schlichtweg davor zurück, ein bestehendes System durch ein neues zu ersetzen. Zudem waren Cyberangriffe längst noch nicht auf dem Niveau, das sie heute haben. IT-Security erschien manchem Verantwortlichen daher eher als Kostenstelle denn als Zugewinn.

Zero Trust erfordert letztlich eine drastische Änderung des kompletten Sicherheitsansatzes. Die Absicherung jeder einzelnen Entität verlangt ein viel breiteres Know-how des IT-Security-Teams und sorgt gleichzeitig für tägliche Mehrarbeit. Dies führt zwangsläufig zu einem erhöhten Bedarf an Fachkräften, die sich darum kümmern müssen. Oder an Sicherungslösungen, die mit Machine Learning und Prozessautomatismus zumindest Teilarbeiten ausführen. Bereits 2010 waren Security-Experten Mangelware, heute sieht es nicht anders aus. Der Einsatz Künstlicher Intelligenz, wie sie heute in immer mehr Lösungen erst im Kommen ist, war in der jüngeren Vergangenheit eher Wunschdenken als in der Realität gewinnbringend nutzbar.

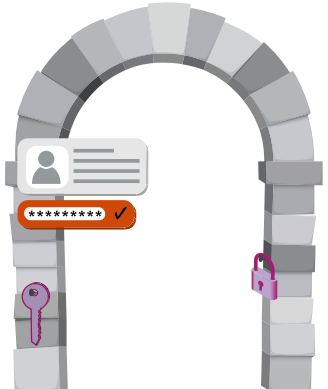
Wie sich später herausstellte, standen viele Organisationsmitglieder Zero Trust aus einem allzu menschlichen Grund negativ gegenüber: Sie fühlten sich an den Pranger gestellt, denn der Mensch gilt als das größte Sicherheitsrisikio und somit der Mitarbeiter selbst. Viele fühlten sich vorverurteilt, bemängelten das vermeintlich fehlende Vertrauen (Trust) der Führung in das eigene Können. Auch wenn das eine mit dem anderen wenig zu tun hat, konnte diese Haltung nicht aufgelöst werden. Die unglückliche Kommunikation bei der Einführung und Erklärung des Begriffs Zero Trust hielt sich hartnäckig in den Köpfen.

Abgesehen von den beschriebenen Problemen kamen ganz pragmatische im Arbeitsalltag hinzu, die direkt mit Zero Trust und dessen Prinzipien bei der Umsetzung verknüpft sind:

- **Alle Datenquellen und -dienste werden als Ressourcen betrachtet** - Das Hauptproblem besteht in der Identifizierung von Datenquellen und -diensten im Unternehmen. Inzwischen haben sich sowohl interne als auch externe Datenquellen gleichwertig etabliert. Und davon existieren inzwischen hunderte, wenn nicht gar tausende, die im Netzwerk aufgerufen werden. Dies führt zu dem für Administratoren ungemütlichen Zustand, dass sich diese Wissensressourcen im Laufe der Zeit permanent verändern. Es entstehen aktualisierte, gänzlich neue und alte werden inaktiv oder existieren nicht mehr. Die Identifizierung der Ressourcen verlangt nach einem ständigen Prozess, der in der Praxis aber teuer ist.

- **Geringste Berechtigung wird zur Durchführung einer Aktion gewährt** - Der Zugriff auf Daten und Anwendungen sollte nur für die Durchführung der erforderlichen Operationen beschränkt werden. Die Umsetzung der Limitierung birgt aber diverse Probleme, angefangen bei der exakten Definition der für die Durchführung von Aktionen erforderlichen Berechtigungen. Dies könnte sich auch negativ auf die Benutzererfahrung auswirken oder unterschiedliche Ressourcen, Ansätze und Werkzeuge erfordern. Der „Least Privilege"-Ansatz verringert auch die Offenheit und den Informationsaustausch in der Organisation, was sich ebenfalls negativ auf die Zusammenarbeit zwischen Mitarbeitern oder Abteilungen auswirken kann.

- **Der Zugriff auf Ressourcen wird pro Sitzung gewährt** - Unter einer Sitzung versteht man landläufig die Zeit, in welcher der Benutzer eine aktive Arbeit ausführt. Doch was passiert, wenn Sitzungen zeitlich begrenzt, die Aktionen aber noch nicht beendet sind? Oder wenn Aufgaben kurzfristig unterbrochen werden müssen, die Session aber durch die Pause automatisch stoppt? Darüber hinaus gibt es in Unternehmen einen hohen Automatisierungsgrad, bei dem ständig Daten verarbeitet werden und die Sitzungen unbegrenzt sein müssen. Die Variabilität der Aufgaben und die individuellen Arbeitsweisen eines jeden Mitarbeiters können kaum in vernünftige Regeln gegossen werden.



- **Der Zugriff auf Ressourcen wird durch dynamische Richtlinien bestimmt** - Zunächst benötigen Unternehmen geeignete Werkzeuge, um Richtlinien festzulegen und durchzusetzen. Dies kann in komplexen hybriden Umgebungen schwer zu verwalten und obendrein teuer sein. Sobald diese Leitlinien jedoch dynamisch anzuwenden sind, müssen sie transparent sein. Nur dann können im Falle eines abgelehnten Zugriffs die Gründe dafür nachvollzogen werden. Die Notwendigkeit der Erklärbarkeit reduziert den Einsatz von Künstlicher Intelligenz, die oft in Blackbox-Manier agiert.

- **Die Organisation überwacht und misst die Integrität und die Sicherheitslage aller eigenen und zugehörigen Vermögenswerte** - Mangelndes Vertrauen und auch die daraus resultierende Überwachung sind mit hohen Kosten verbunden. Fast jeder einzelne Vermögenswert in einem Unternehmen kann kompromittiert werden - und besitzt heutzutage eine große Komplexität. Selbst ein einzelnes Gerät ist mit seinen internen Software- und Hardwarekomponenten so umfassend, dass die Organisation nicht immer in der Lage ist, seine Integrität und Sicherheit komplett zu überprüfen.

- **Die Organisation sammelt so viele Informationen wie möglich, um ihre Sicherheitslage zu verbessern** - Daten sollten nicht nur gesammelt, sondern auch analysiert und ausgewertet werden. Dies erfordert Speicherplatz, Werkzeuge und ausreichend qualifizierte Arbeitskräfte, um sie gewinnbringend nutzen zu können. Das verfügbare Budget stellt dabei oft das Haupthindernis dar.

WAS TREIBT DAS ERNEUTE INTERESSE AM ZERO TRUST-MODELL UND AN DESSEN EINFÜHRUNG AN?

Aus Schaden wird man klug: Dieses uralte Sprichwort beschreibt den Grund für die Renaissance von Zero Trust vielleicht am besten. Denn in den letzten Jahren kamen Perimeter-basierte Netzwerkarchitekturen böse unter die Cybercrime-Räder. Ransomware und Advanced Persistant Threats (APT) zeigten den IT-Sicherheitsteams unmissverständlich, wo die Grenzen ihrer Sicherheitsstrukturen lagen und liegen. Ob Regierungen, Militärs, Konzerne oder Kritische Infrastrukturen: Es verging quasi kein Tag, an dem nicht über einen spektakulären Hackerangriff auf die Big Player in den Medien berichtet wurde. Immer wieder zeigte sich während der forensischen Analyse der Vorfälle, dass Sicherheitslücken nicht erkannt oder nicht für ernst genommen oder Angriffsflächen den Hackern kaum gesichert geboten wurden.

Die Folgen waren für viele Betroffene dramatisch und gingen richtig ins Geld. Die Erhebung „2020 Cost of a Data Breach Report" von IBM und dem Ponemon Institute ergab, dass die durchschnittlichen Kosten einer Datenschutzverletzung weltweit bei 3,86 Millionen US-Dollar lagen. Die durchschnittliche Zeit zur Identifizierung und Eindämmung einer Verletzung betrug sagenhafte 280 Tage. Zusätzlich durften viele EU-Unternehmen empfindliche Strafen bezahlen, denn Sicherheitsvorfälle gehen zumeist Hand in Hand mit Datenschutzverletzungen. Da verstehen die Behörden der Datenschutzgrundverordnung (DSGVO) keinen Spaß.

Weitere Analysen zeigen eindrucksvoll, dass Zero Trust-Umgebungen viele dieser erfolgreichen Hackerangriffe abgewehrt hätten. Mit ihrer Kontrolle und dem Wissen über alle eigenen Daten wären Sicherheitsverstöße schneller erkannt worden oder im schlimmsten Fall klar gewesen, wann und wo Angreifer Informationen gestohlen haben. Allein vor diesem Hintergrund erscheint das Zero Trust-Modell recht attraktiv.

Auf der anderen Seite stehen mit dem IT-Dauerbrenner „Bring your own device" (BYOD) und dem rasanten Wachstum von „Remote Work" zwei dicke Brocken auf der Dauerprioritätenliste. Denn immer mehr Mitarbeiter möchten von jedem Ort und zu jeder Zeit Zugriff auf die internen Ressourcen ihrer Organisation haben – und das mit den von ihnen präferierten Mitteln. Eine weitere Komponente,

die Zero Trust vorantreibt, ist die zunehmende Akzeptanz und Nutzung von Speicherdiensten in der Cloud. Diese hostet oft die Daten, Ressourcen und sogar die kritischen Dienste von Unternehmen. Zu all diesen Aspekten können perimetergetriebene Strukturen keine zukunftsweisenden Security-Antworten geben.

Figure 2: Top-Gefahren in 2022. Quelle: ENISA, Threat Landscape 2021

CORONA ALS GAME CHANGER

Zur post-pandemischen Normalität von Organisationen werden in Zukunft die verstärkte Nutzung digitaler Technologien und flexiblere Arbeitsmodelle gehören. Doch obwohl Technologiegiganten wie Twitter und Facebook Schlagzeilen mit dem Versprechen machten, dass einige Mitarbeiter für immer von zu Hause aus arbeiten können, ist die Realität für die meisten Arbeitgeber wahrscheinlich weniger klar. Aktuellen Studien zufolge planen mehr als 60 Prozent der befragten

Unternehmen, hybride Arbeitsmodelle einzuführen, bei denen die Mitarbeiter einen Teil der Woche zu Hause und einige Tage im Büro verbringen. Damit werden zweifelsfrei neue Cyber-Risiken einhergehen.

Genau für diesen Fall wurde das Zero Trust-Modell entwickelt, das beispielsweise in einer neuen Präsidialverordnung von US-Präsident Biden bereits für US-Bundesbehörden vorgeschrieben wurde. Es erlaubt Organisationen in einer Welt mit flexiblen Arbeitsmodellen, Cloud-Architekturen und hartnäckigen Bedrohungsakteuren Cyber-Risiken zu minimieren. Damit könnten US-amerikanische Organisationen als Vorzeigeobjekte in puncto perimeterlose IT-Security-Modelle fungieren.

CISOs von heute stehen unter unglaublichem Druck, Geschäftsgeheimnisse und Kundendaten vor Diebstahl und geschäftskritische Systeme vor Service-Unterbrechungen zu schützen. Durch die massenhafte Fernarbeit und die zunehmenden hybriden Arbeitsplätze entstehen für Hacker noch mehr Vorteile. Deshalb müssen Verantwortliche ihre Hausaufgaben machen: Aktuelle Probleme in und durch Home-Offices kommen auch auf Zero Trust-Architekturen zu. Hier ein paar Beispiele:

- Abgelenkte Heimarbeiter, die eher auf Phishing-Links hereinfallen
- Remote-Mitarbeiter, die möglicherweise unsichere private Laptops und mobile Geräte, Netzwerke und Smart-Home-Geräte für die Arbeit verwenden
- Angreifbare Virtual Private Networks (VPN) und andere ungepatchte Software,
  die auf Heim-Systemen ausgeführt wird
- Schlecht konfigurierte Remote Desktop Protocol (RDP) Verbindungen auf Endpoints, die leicht über geleakte oder leicht zu erratende Passwörter gekapert werden können
- Cloud-Dienste mit schwachen Zugriffskontrollen (schlechte Passwörter und keine Multi-Faktor-Authentifizierung)

Teil 3:

ESETs Idee von Zero Trust „reloaded“

ESET FORDERT EINEN PARADIGMENWECHSEL IN PUNCTO IT-SECURITY

Die Bedrohung durch Cyberkriminelle ist in Deutschland nach Einschätzung des Bundeskriminalamts (BKA) weiter angestiegen. Im kürzlich vorgelegten „Lagebild Cybercrime 2021" zeichnen die Experten ein düsteres Bild. So steigt nicht nur die Anzahl der Angriffe, sondern ebenso die Qualität in gefährlichem Maße permanent an. Und dass Ransomware die aktuell größte Gefahr darstellt, überrascht niemanden mehr wirklich.

Die Lehre aus den vielen Vorfällen der letzten Monate ist bitter, aber durchaus hilfreich. Wer Software und Anwendungen mit all ihren nützlichen Funktionen für sein Unternehmen nutzen will, kann die Augen nicht vor den immer größer werdenden Gefahren verschließen, sondern muss umdenken.

- Es reicht nicht mehr aus, dass Administratoren möglichst schnell auf neue Bedrohungen reagieren. Wenn sie eingreifen, ist es vielleicht schon zu spät.

- Es reicht nicht mehr aus, mit Antivirensoftware, Spam- und Phishingfilter und Firewall die Angriffe abwehren zu wollen. Dafür sind diese zu raffiniert und vehement.

- Es reicht nicht mehr aus, das eigene Netzwerk im Bürogebäude als „sicher und ungefährlich" anzusehen und nur alles Externe als Bedrohung aufzufassen.

Die Frage ist heutzutage nicht mehr, ob es zu einem Angriff kommt, sondern wann. Geschehen wird er in jedem Fall. Diese Einsicht ist wesentlich für einen Paradigmenwechsel in Organisationen. Diese benötigen fachkundige Exchange-Administratoren, Security-Lösungen, ein internes Sicherheitsteam oder einen externen Managed Service Provider nicht als Selbstzweck, um ein gutes Gewissen zu haben. Man muss sich ernsthaft und proaktiv auf Cyberattacken vorbereiten. Und sich fragen, welche Schwachstellen im eigenen Unternehmen existieren und abgesichert werden müssen.

Aus diesem Grund ist es essenziell, sich proaktiv auf Cyberattacken vorzubereiten. Denn Firewall, Antivirenlösungen und Co. sind „nur" reaktive Module. Sie kommen

erst zum Einsatz, wenn der Angriff auf die eigenen Systeme läuft. Damit kann man aber nicht ausschließen, dass sich nicht schon Malware im eigenen Netzwerk befindet, die beispielsweise unbemerkt über Sicherheitslücken hereingekommen ist. Oder noch schlimmer: Wenn Fremde über gekaperte Zugangsdaten einen Weg ins Netzwerk gefunden haben.

PERIMETER DEFENSE SECURITY HAT AUSGEDIENT

ESET sieht in Zero Trust ein Sicherheitsmodell, das zu Recht und zunehmend an Popularität gewinnt. Das bislang übliche Perimeter Defense Modell hat nach Meinung des IT-Sicherheitsexperten seinen Zenit überschritten und gehört abgelöst. Die langjährige Security-Systematik beruhte (wie zuvor beschrieben) auf die Anwesenheit der Mitarbeiter in den eigenen vier Bürowänden - gut gesichert durch die firmeneigene IT. Heute greifen aber immer mehr Angestellte, externe Dienstleister sowie Geschäftspartner von verschiedenen Orten auf Daten und Dienste zu. Immer mehr Anwendungen werden im SaaS-Modell (Software-as-a-Service) bereitgestellt. Mitarbeiter greifen direkt auf sie zu, ohne einen VPN-Tunnel zum Unternehmen aufzubauen. Was ein Perimeter in modernen Organisationen ist, lässt sich oft nicht einmal definieren. Kurzum: Es ist nicht einfach, die Sicherheit in einer modernen, komplexen Umgebung zu gewährleisten. Es gibt keine „vertrauenswürdigen Zonen" mehr, die es zu sichern gilt. Vielmehr muss die Sicherheit für jede einzelne Entität, die mit Unternehmensressourcen in Kontakt steht, gelten und permanent überprüft werden. Sie dürfen nur für eine begrenzte Zeit und auf diejenigen Ressourcen gewährt werden, die für die Durchführung der erwarteten Aktion erforderlich sind.

WARUM SETZT ESET AUF ZERO TRUST?

Ein moderner Zero Trust-Ansatz spiegelt die Sicherheitsbedürfnisse von Organisationen viel besser wider als ältere Sicherheitsmodelle. Mit der Zeit wird er sich in der digitalen Welt durchsetzen, auch wenn die Umsetzung für manche schwierig und kostspielig sein wird. Doch die Alternative, den Status Quo zu behalten, dürfte deutlich teurer werden, wenn Hackerangriffe zum Ziel führen. Finanzielle Schäden, Reputationsverlust und vermutlich auch Strafen durch Verstöße gegen die Datenschutzgrundverordnung gehen richtig ins Geld, Insolvenz nicht ausgeschlossen. Mit der Verlagerung von Infrastrukturen und Diensten in die Cloud ändert sich nicht nur die Angriffsfläche, sondern sie

vergrößert sich auch. Denn nur die wenigsten Unternehmen arbeiten rein Cloud-basiert: Viele betreiben auch in Zukunft einen Mix aus Kerngeschäft in den eignen Räumlichkeiten, Cloud-Diensten, externen Arbeitsplätzen und Dienstleistern.

Zero Trust kann zu einer erhöhten Sicherheit von Organisationen führen. Administratoren, Informationsbeauftragte und Sicherheitsingenieure haben die Chance, das Security-Niveau den Herausforderungen anzupassen, neue Sicherheitsrichtlinien festzulegen, Schwachstellen zu identifizieren und diese entweder zu beseitigen oder durch neue Prozesse und Tools zu härten. Der Hype um Zero Trust muss die Budgetverantwortlichen und Unternehmenslenker erreichen und mitnehmen, damit die erforderlichen Ressourcen und die Zeit für die Sicherheit bereitgestellt werden.

NEUER DENKANSATZ: ESET ZERO TRUST SECURITY

Wie lässt sich nun in der Praxis „proaktiv" agieren und Sicherheit neu denken? Vom Prinzip her stellt sich nur eine Frage: Wie kommen Cyberkriminelle überhaupt ins eigene Netzwerk? Die Antwort darauf ist schon die Lösung. Wenn man das Patch Management für Betriebssysteme und Software als „Muss" ausklammert, bleiben eigentlich nur noch vier Bereiche für Angreifer übrig: unsichere Datenverbindungen, keine eindeutige Überprüfung der Identitäten von Mitarbeitern, Malware und der Risikofaktor Mensch (speziell Phishing und Social Engineering).

Diese wunden Punkte haben Administratoren eigentlich im Blick, allerdings ist deren Denkgerüst dahinter vielfach ein nicht mehr zeitgemäßes - und lautet ungefähr so: Alles, was sich im eigenen Netzwerk (und auch im selben Bürogebäude) befindet, kann man als eher sicher und gefahrenfrei einschätzen. Alles, was von außen hereinkommt, sollte einer gründlichen Überprüfung unterzogen werden. Das war bis vor kurzem absolut richtig und ausreichend. In Zeiten von Corona, Home-Office und starker Digitalisierung passt die Methodik nicht mehr so gut. Denn immer mehr Mitarbeiter, die vor kurzem noch „innen" waren, sind plötzlich extern im Home-Office. Trotzdem werden sie nicht ausreichend als potenziell gefährlich eingeschätzt. Wer sich zum Beispiel über eine RDP-Verbindung am Firmenserver einwählt und die richtige Kombination aus Benutzername und Passwort kennt, der muss ja freundlich sein.

An diesem Punkt kommen Hacker ins Spiel: Genau das wissen die Täter und attackieren äußerst zielgerichtet. So ist es kein Wunder, dass sich die Angriffe auf das Remote Desktop Protocol (RDP) konzentrieren. Mit Erfolg: ESET identifizierte zwischen 2020/2021 71 Milliarden Angriffsversuche auf die RDP-Verbindungen, welche die Mitarbeiter im Home-Office mit ihren Unternehmensnetzwerken verknüpft. Im Erfolgsfall stehen nur noch Benutzername/Passwort als Hürde im Weg. Das Knacken dieser Kombination per Brute Force, durch im Darknet illegal erworbener Zugangsinformationen oder Datenbankangriffe gehören zur Basisausstattung moderner eCrime-Banden. Auch Phishing- und Malware-Attacken verzeichnen ähnlich hohe Zahlen, denn das Home-Office ist in vielen Fällen nicht so abgesichert, wie es hätte sein sollen.

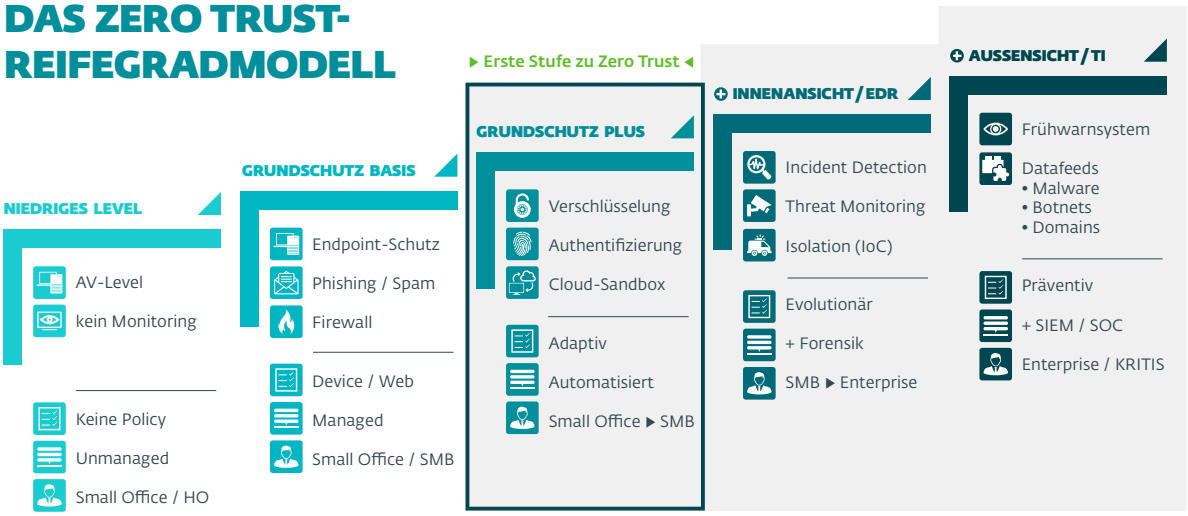
Vorausschauendes Denken bedeutet in diesem Punkt für jede Organisation, es „Eindringlingen" so schwer wie möglich machen. Daher sollten sie ein Virtual Private Network (VPN) anstelle einer RDP-Verbindung und eine Multi-Faktor-Authentifizierung implementieren, um Internetzugriffe auf Server besser abzusichern. Oder anders gesagt: Wer von extern in das Netzwerk eintreten möchte, muss nachweisen, dass er dies über den richtigen, abgesicherten Weg vornimmt und gleichzeitig die Person ist, die er vorgibt zu sein. Hinzu kommt noch eine weitere zu berücksichtigende und bislang oft vernachlässigte Tatsache: Im eigenen Netzwerk laufen zu wenige Kontrollen, ob sich nicht doch etwas oder jemand eingeschlichen hat, der das System gefährden könnte.

DAS ESET REIFEGRADMODELL

Nimmt man den letzten Punkt hinzu, gelangt man zum Denkansatz von „Zero Trust Security". Diese konzeptionelle Basis hat ESET aufgegriffen, weiterentwickelt und auf die Bedürfnisse unterschiedlicher Organisationsgrößen zugeschnitten. In Zeiten von Corona und Home-Office hat sich das als zwingend erforderlich erwiesen. Der Zero Trust Security-Ansatz von ESET besteht aus einem dreistufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer". Das Modell startet mit der Basisstufe „Grundschutz Plus", die dem Prinzip des „Multi Secured Endpoint" folgt. Diese eignet sich unabhängig vom individuellen Schutzbedarf für jede Organisation und sollte die Mindestanforderung jeder IT-Abteilung abbilden. Daran schließen sich zwei Zero Trust-Stufen mit weiter steigenden Security-Maßnahmen und -Diensten an.

Eine der großen Herausforderungen stellen Insellösungen dar, die nicht verzahnt ineinandergreifen. ESET hat dies frühzeitig erkannt und bietet mit seinem „Multi Secured Endpoint"-Ansatz ein am Markt einmaliges Lösungsportfolio an, das technologisch ausgereift ist und umfassend das nötige Schutzniveau gewährleistet. Der europäische Hersteller setzt dabei konsequent auf eigene Technologien – und das über alle gängigen Betriebssysteme hinweg, cloudbasiert oder on-premises. Von der Endpoint Protection über die Multi-Faktor-Authentifizierung bis hin zur Verschlüsselung können Kunden auf ESET vertrauen. Das sogenannte „Single Vendor Prinzip" vereinfacht es den Administratoren und reduziert zugleich den Kostenaufwand. Nahezu alle ESET Lösungen lassen sich über die Management-Konsole ESET PROTECT komplett administrieren.

Die Sicherheit aus einem Guss basiert auf dem Bekenntnis zu Zero Trust Security, also dem vollumfänglichen Schutz aller Geräte, sowohl intern als auch extern. Damit geht ESET sogar einen Schritt weiter, als es das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert. Dies ist insbesondere für alle Organisationen und Unternehmen wichtig, die als Kritische Infrastrukturen (KRITIS) eingestuft sind.



Basisstufe:
Der Multi Secured Endpoint sichert den Alltag ab

Natürlich hat nicht jedes Unternehmen oder jede Institution die Ressourcen, komplett und sofort auf Zero Trust Security umzuschwenken. Enorme finanzielle und personelle Investitionen in Threat Intelligence-Tools oder Endpoint Detection and Response (EDR)-Lösungen lohnen sich für sie nicht. Das ist in vielen Fällen aber auch nicht erforderlich.

Mit dem sogenannten Multi Secured Endpoint legen IT-Verantwortliche einen wichtigen ersten Grundstein von Zero Trust Security. Dieser sichert so Endpoints weit besser ab als andere Systematiken zuvor. Und: Es spielt nun keine Rolle mehr, ob sich das Gerät oder der Anwender im IT-sicheren Bürogebäude befindet. Im Zusammenspiel vom vorhandenen Malware-Schutz mit einer Festplattenverschlüsselungs- und Multi-Faktor-Authentifizierungslösung sowie Cloud Sandboxing verwandeln Administratoren PCs und Laptops in sogenannte „gehärtete Endpoints". Diese benötigen keine Serverstrukturen oder Verbindungen zum Netzwerk, um optimal gesichert zu sein.

VERSCHLÜSSELUNG STOPPT DATENSCHNÜFFLER

Alle auf dem Endpoint gespeicherten Informationen sollten vor neugierigen Blicken oder im Verlustfall geschützt sein. Mit dem Einsatz einer Verschlüsselung schlagen Verantwortliche zwei Fliegen mit einer Klappe. Cyberkriminelle können mit den codierten Daten nichts anfangen und gleichzeitig kommt das Unternehmen Anforderungen aus der Datenschutzgrundverordnung nach. Voraussetzung für den Erfolg der Verschlüsselung ist die Akzeptanz des Anwenders. Deswegen sollte die Lösung bei ihrer täglichen Arbeit kaum „spürbar" und zuverlässig arbeiten.

CLOUD SANDBOXING HÄLT DAS POSTFACH SAUBER

Das Entdecken schädlicher E-Mails und deren Anhänge oder Downloads ist ein wichtiger Eckpfeiler für optimale Sicherheit. Gerade der Empfang von Office-

Dokumenten, PDFs und zuweilen auch ausführbaren Dateien gehören zum Alltag in Büros. Nichts wäre schlimmer, als wenn durch dieses Schlupfloch beispielsweise Ransomware eindringt, alle Daten ungewollt verschlüsselt und unzugänglich macht. Abhilfe schaffen in diesem Punkt Lösungen mit einer cloudbasierten Sandbox. Suspekter und potenziell gefährlicher Binärcode wie Ransomware, Advanced Persistent Threats und Exploits wird in einer gesicherten Umgebung ausgeführt und erst bei negativem Befund in das Postfach übermittelt.

DATEN- UND NETZWERKZUGRIFF NUR MIT MULTI-FAKTOR-AUTHENTIFIZIERUNG

Für jeden Administrator ist es ein Albtraum, wenn sich jemand ins Netzwerk einloggt oder Daten aufruft, dessen Identität nicht eindeutig geklärt ist. Deshalb sollte eine Multi-Faktor-Authentifizierung grundsätzlich implementiert werden. Es befindet sich eine Reihe von Lösungen auf dem Markt, die einfach zu handhaben und kostengünstig in der Anschaffung sind. Beispielsweise ebnen professionelle Softwareprodukte den sicheren Zugang zu sensiblen Informationen und Netzwerkumgebungen. So lassen sich in weniger als einer Viertelstunde komplette Netzwerke mit tausenden von Rechnern ausstatten. Zusätzliche Hardware-Anschaffungen sind unnötig, bestehende Smartphones lassen sich per App, FIDO-Sticks oder andere Token problemlos integrieren.

Ausbaustufe Innenansicht: **Endpoint Detection and Response**

Hackerattacken erfolgen in den seltensten Fällen „Knall auf Fall". Frontalangriffe, wie sie noch vor wenigen Jahren die Regel waren, finden immer seltener statt. Denn die eingesetzten Security-Lösungen sind darauf bestens vorbereitet und wehren diese in den meisten Fällen ab. Je besser das anzugreifende Netzwerk jedoch abgesichert ist, desto intensiver müssen Cyberkriminelle nach Schwachstellen suchen. Und geeignete Wege finden, um in der Organisation eine Basis für einen Angriff schaffen zu können. Dazu zählen beispielsweise Zugänge zu sensiblen Bereichen zu ergaunern oder scheinbar harmlose Dateien einzuschleusen, die erst im Zusammenspiel ihre toxische Wirkung entfalten. Insbesondere, wenn Advanced Persitent Threats und Zero Day Exploits ins Spiel kommen, stoßen klassische Sicherheitsprodukte an ihre Grenzen. Diese Gefahren können selten direkt, wie beispielsweise Malware, erkannt werden, verraten sich aber über ihre spätere Arbeitsweise im Netzwerk.

VERRÄTERISCHE ANOMALIEN ENTDECKEN

Und genau auf diese Veränderungen an Dateien, Protokollen und ausgeführten Diensten springen die sogenannten Endpoint Detection and Response-Lösungen (EDR) beinahe in Echtzeit an – und könnten sofort überprüft werden. Und sie bieten eine weitere wichtige Einsatzmöglichkeit: Anhand von EDR können nach einer Cyberattacke forensische Untersuchungen eingeleitet werden. Ähnlich einem Mordfall in bekannten Krimis werden möglichst viele Informationen gesammelt und „Alibis", in diesen Fällen die ordnungsgemäßen Arbeitsweisen, überprüft. Administratoren erkennen dann zuverlässig, wie der Angriff ablief, welche Schwachstellen konkret ausgenutzt und welche Veränderungen im Netzwerk vorgenommen wurden. Dazu kann der Verantwortliche auf Informationen des Reputationssystems ESET LiveGrid zurückgreifen und/oder anhand des MITRE Attack Frameworks die Attacke nachvollziehen. So lassen sich Security-Lecks sofort stopfen und das Gesamtsystem für die Zukunft sicherer gestalten.

ENTDECKEN UND SOFORTIGES HANDELN

Der Begriff „Endpoint Detection and Response" beschreibt die beiden wichtigen Einsatzzwecke. Zum einen soll damit der Endpoint geschützt werden, auf dem die meisten Hacker-Aktivitäten stattfinden. Dort liegt ein Großteil der schutzwürdigen Daten vor bzw. werden am Gerät zum Beispiel Passwörter oder Bankdaten eingegeben. Nicht zu vergessen, lauert am Endpoint einer der größten Risikofaktoren, der Mitarbeiter. Zum anderen beschreibt „Response", dass auf Anomalien sofort reagiert werden kann. Je nachdem kann das eine manuelle Reaktion eines IT-Sicherheitsexperten oder eine automatische, zuvor definierte Verhaltensweise sein.

SO FUNKTIONIERT ENDPOINT DETECTION AND RESPONSE

Mit EDR stehen Administratoren professionelle Technologies zur Seite, die verdächtiges Verhalten und Sicherheitslücken innerhalb des Netzwerks automatisch aufspüren. Alle Aktivitäten innerhalb der IT-Infrastruktur (Nutzer-, Datei-, Prozess-, Registry-, Speicher- und Netzwerk-Vorgänge) können in Echtzeit überwacht und bewertet werden, sodass der IT-Verantwortliche bei Bedarf sofort handeln kann. Nur auf diese Weise lassen sich erste Spuren von Hackern identifizieren, Fehlverhalten von Mitarbeitern bestimmen und Sicherheitsmängel ausfindig machen. Oder wie gesagt, die Einfallstore finden, die bei einem erfolgreichen Hackerangriff auf das eigene Netzwerk zu weit offenstanden. Die kürzlich entdeckten Sicherheitslücken in Microsoft Exchange hätten beispielsweise mit EDR vielleicht nicht komplett gestoppt, aber die Schäden auf ein Mindestmaß reduziert werden können.

Die Auswertung aller Endpoint-Daten in einem Netzwerk lässt Rückschlüsse auf die Validität einzelner Abläufe zu. Eine genaue Erfassung von alltäglichen Vorgängen wie das Kopieren von Dateien, User-Zugriffe auf bestimmte Bereiche im Netzwerk oder aber auch An- und Abmeldungen von Anwendern erlaubt bei entsprechender Auswertung ein Herausfiltern bösartiger Aktivitäten.

EDR-Lösungen ersetzen dabei keine Endpoint Protection oder Antiviren-Lösungen, sondern ergänzen sie um eine wichtige Komponente: die Erkennung von Verhaltensanomalien, die im Netzwerk und auch auf den Endpoints auftreten. Diese Erkennung basiert auf vordefinierten Regeln in einem Rechnerverbund, die

alle legalen Aktivitäten abbilden. Basierend auf diesen Angaben analysiert die EDR-Anwendung die Datenströme. Darüber hinaus werden auch Informationen der eingesetzten Endpoint Protection in die Bewertung einbezogen.

INNENANSICHT ERHÖHT SICHERHEITSNIVEAU

EDR-Systeme helfen Organisationen in puncto Sicherheit eine umfassende Innensicht über ihr System zu erhalten, Datenabflüsse frühzeitig zu stoppen und im Gefahrenfall Anwendungen oder ganze Rechner zu sperren. Der detaillierte Einblick in die Vorgänge im Netzwerk ermöglicht zudem, Probleme zu verstehen und in Zukunft zu verhindern. So lassen sich zum Beispiel verdächtige E-Mail-Anhänge oder bestimmte Netzwerkressourcen für Mitarbeitergruppen sperren. Kostspielige Betriebsstörungen oder sogar -ausfälle lassen sich so proaktiv vermeiden.

Im Moment gibt es nur wenige Hersteller, die EDR-Lösungen im Portfolio haben und auf aktive Nutzer verweisen können. Zu diesen zählt der europäische IT-Security-Spezialist ESET mit seinem Produkt ESET Inspect. Aufgrund der Komplexität von Endpoint Detection and Response nutzen bislang eher große Konzerne solche Lösungen, bei denen die IT-Abteilungen entsprechende Ressourcen und umfassendes Know-how mitbringen. Inzwischen bieten immer mehr Systemhäuser und Managed Security Service Provider fortschrittliches Endpoint Detection and Response als mietbare Dienstleistung an. So erhalten auch mittelständische/ mittelgroße Unternehmen die Möglichkeit, diese wichtige Sicherheitsmaßnahme einzusetzen.

Alternativ können Unternehmen, für die EDR noch nicht in Frage kommt, auf umfassende Security-Dienstleistungen setzen. Diese bieten Hersteller von Sicherheitslösungen, aber auch Fachhändler und Systemhäuser an. Darunter zählen Premium Support Services, die bei Problemen im Alltag schnelle Lösungen erarbeiten. Oder eben Security Services, die neben Incidient Response auch digitale Forensik und EDR abdecken. Anbieter wie ESET satteln mit „Managed Detection and Response“ noch einen drauf. Dies umfasst alle Funktionalitäten und Dienstleistungen von Security Services und erweitern die eingesetzten ESET Lösungen um Threat Monitoring, Threat Hunting sowie Deployment & Upgrade.

Ausbaustufe Außensicht: **Threat Intelligence**

Abwehrmaßnahmen gegen Malware und Hacker ergreifen zu können, bevor sie zuschlagen: Davon träumen Administratoren und IT-Sicherheitsbeauftragte. Mit „Threat Intelligence" kommen sie dem Ideal ein gehöriges Stück näher. Security-Experten wie ESET sammeln über ihre Sensoren weltweit Informationen zu Malware-Vorfällen und Angriffen, werten diese aus, erstellen eine Gefahrenanalyse und geben konkrete Handlungsempfehlungen. Verantwortliche können bereits reagieren, bevor der eigentliche Impact stattfindet.

REAGIEREN, BEVOR ES „KRACHT"

Jede Sekunde zählt – diese Tatsache gilt für drohende Tsunamis genauso wie für Cyber-Bedrohungen. Gewissermaßen hat das Riesenwellen-Frühwarnsystem Pate gestanden für ESET Threat Intelligence. Beide Systeme schützen ihre Empfänger, indem sie ihnen einen zeitlichen Vorsprung verschaffen, um sich in Sicherheit zu bringen oder zumindest für die Abwehr bereit zu machen. Dieser Puffer ist wichtiger denn je. Cyberkriminelle rüsten ihre Malware und andere Werkzeuge permanent auf. Die immer komplexer werdenden Angriffe treffen Unternehmen oftmals quasi aus dem Nichts. Security-Beauftragten bleibt letztlich nur die Möglichkeit zu reagieren und zu hoffen, dass die eingesetzten Security-Lösungen der Cyberattacke standhalten.

INFORMATIONSGEWINNUNG À LA JAMES BOND

Genau hier setzt die Idee von Threat Intelligence an. Zusätzlich zum proaktiven Schutzschirm der IT-Sicherheit installiert man einen weiteren Schild, der – vereinfacht gesagt – wie ein Geheimdienst permanent aktiv nach neuen Bedrohungen Ausschau hält und Auswertungen bekannter Vorfälle vornimmt. Denn Cyberkrimelle hinterlassen zwangsläufig Spuren, wenn sie Malware versenden, ihre Botnets aktivieren oder zielgerichtete Angriffe fahren. IT-Verantwortliche, die einzig und allein Zugang zu internen Daten haben, können diese gewaltige Aufgabe gar nicht bewältigen.

MEHR SICHERHEIT DURCH BIG DATA

ESET Threat Intelligence schließt also die Lücke zwischen den Informationen aus dem Kundennetzwerk und den von ESET gesammelten Daten aus der digitalen Welt. Der Sicherheitsspezialist nutzt die von mehr als 110 Millionen Sensoren weltweit über ESET LiveGrid erfassten Informationen, die an das cloudbasierte Sicherheitssystem übermittelt werden. Dazu zählen beispielsweise Malware-Funde, geblockte oder erfolgreiche Angriffe oder Phishing-Mails. In den Forschungs- und Entwicklungszentren rund um den Globus sichten und werten Spezialisten diese Daten aus. Zusätzlich werden sowohl interne als auch externe Datenquellen (aktuelle weltweite Bedrohungslandschaft sowie typische Angriffsvektoren und -ziele) zusammengeführt.

Dabei arbeiten menschliche Expertise und Machine Learning Hand in Hand. So ist ESET in der Lage, mit tagesaktuellen Daten seinen Kunden ein enormes und besonderes Wissen zur Verfügung zu stellen. Das Ziel: Risiken besser zu verstehen und auf Bedrohungen effektiv zu reagieren.

DREI TYPISCHE USE CASES

1. Unternehmen können mit den speziell für sie zugeschnittenen Informationen erkennen, ob sie oder deren Kundenstamm Ziel einer Attacke oder mehrerer Angriffe sind und welche Gegenmaßnahmen erforderlich sind.

2. Ein Unternehmen kann zum Beispiel erkennen, ob in seinem Namen Phishing-Mails an Endkunden versandt werden und proaktiv warnen. Administratoren sehen, welche Angriffe gegen das eigene Netzwerk gefahren werden und können bessere Präventivmaßnahmen treffen.

3. Durch unterschiedliche, von ESET generierte Reports ergeben sich weitere Dienstleistungsmöglichkeiten für Security Operation Center (SOC).

AUSSAGEKRÄFTIGE REPORTS FÜR SCHNELLE REAKTION

Der Clou von Threat Intelligence ist die sinnvolle Kategorisierung und Bündelung aller zur Verfügung stehenden Informationen. Die ESET Lösung bietet eine Reihe von Protokollen: So liefert beispielsweise der Report zu Botnet-Aktivitäten quantitative Daten über bekannte Malware-Familien und Botnet-Varianten. Zudem erhalten Administratoren Informationen über bekannte, in Botnet-Kampagnen eingesetzte Command and Control (C&C) Server, Samples von Botnets, wöchentliche globale Statistiken und eine Liste an Zielen der Malware.
Ein weiterer Report fasst Erkenntnisse zu zielgerichteten Angriffen zusammen. Dieser informiert den Anwender über mögliche aufkommende oder gezielte Advanced Persistent Threats gegen das Unternehmen.
Am häufigsten nutzen ESET Kunden den Bericht zu erkannter Malware. Dieser hält Anwender kontinuierlich über aktuell stattfindende und potenzielle Angriffskampagnen auf dem Laufenden – selbst wenn diese noch am Anfang stehen. Dies geschieht unter anderem auf Basis von YARA-Regelketten, Reputationsinformationen, Binärdateien, Dateieigenschaften und Sandbox-Output.
Über die integrierte API lassen sich Berichte, YARA-Regeln und andere Funktionalitäten auch in bestehende Systeme übertragen.

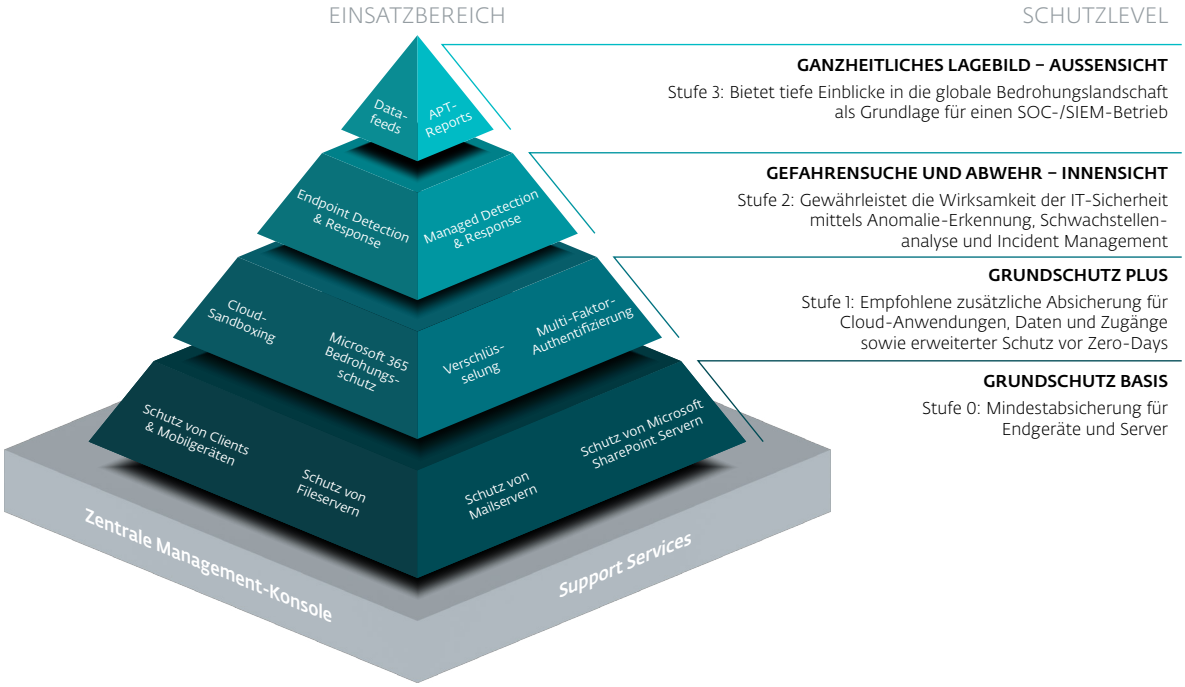
ECHTZEIT DATEN-FEEDS

Zudem bietet ESET Threat Intelligence eine Reihe von Datenfeeds im STIX/TAXII-Format an, die sich einfach in bestehende SIEM-Tools integrieren lassen: u.a. Botnet-Feed, Malware-Feed und Domain-Feed.

Von der Theorie zur konkreten Umsetzung

Die spannende Frage lautet nun: Wie kann ich mein Netzwerk im Sinne von Zero Trust umgestalten? Die ESET Experten haben dazu eine Security-Pyramide – in Anlehnung an die bekannte Ernährungspyramide – erstellt. Jeder Sicherheitsstufe wurden dabei die wichtigsten Gruppen von Security-Lösungen zugeordnet.

Alles beginnt mit der Basis, die unbedingt zu empfehlen ist. Dann folgen weitere Ebenen, die aufeinander aufbauen und das Sicherheitsniveau sukzessive erweitern. Dabei handelt es sich um Empfehlungen, die nicht stur umgesetzt werden müssen. Wer beispielsweise keine Clouddienste von Microsoft benutzt, muss entsprechend keinen Microsoft 365-Bedrohungsschutz einsetzen. Man muss auch nicht alle Sicherheitsprodukte von einem Hersteller beziehen und kann den vielleicht schon gewählten Multi-Vendor-Ansatz beibehalten. Die Praxis zeigt aber, dass alles aus einer Hand (Single-Vendor-Prinzip) oftmals günstiger und leichter zu administrieren ist.



Selbstverständlich gibt es noch viele andere Security-Lösungen, die ebenfalls eingesetzt werden können. Ob Patch Management, Schutz vor DDoS-Attacken oder VPN-Verbindungen – der Zweck heiligt die Mittel. Zero Trust heißt, die Schwächen zu erkennen und Maßnahmen zu ergreifen. Idealerweise, bevor Hacker Schwachstellen ausgenutzt haben.

Fazit

Die gute Nachricht zum Schluss: Mit dem von ESET entwickelten Zero Trust Security-Ansatz „Reifegradmodell" erhalten Organisationen jeglicher Größe eine praxisnahe Methodik an die Hand, um ihre IT-Infrastruktur auf das erforderliche Schutzniveau zu bringen. IT-Verantwortliche und Geschäftsführer können so sicherstellen, dass alle Daten, Anwendungen und Server auch vor unbekannten Schwachstellen bestmöglich geschützt sind. Dann ist schnelles Handeln tatsächlich möglich und Gefahren lassen sich rechtzeitig abwenden. Die nächste Warnung vom BSI ist in dem Fall keine unternehmensbedrohliche Nachricht mehr, sondern lediglich eine nützliche Meldung.

Der Einstieg in Zero Trust fällt vielen Organisationen leichter, als es zuerst den Anschein hat. Denn die vorhandene IT-Sicherheitsarchitektur müsste vermutlich „nur" angepasst werden. Die eingesetzten Securitylösungen bleiben ja bestehen, werden nur um sinnvolle Tools wie EDR erweitert. Mehr Arbeit dürfte der Fokus auf Identitäts- und Zugriffsverwaltungsprogramme hervorrufen. Der Schwachpunkt, den Angreifer am häufigsten ausnutzen, sind vollständig fehlende oder falsch konfigurierte Authentifizierungs- und Autorisierungskontrollen. Identitäts- und Zugriffsverwaltungstechnologien stellen die Steuerebene für Zero Trust-Architekturen dar. Zero Trust-Befürworter bauen ihre Umgebungen heute so auf, dass sie mit der strategischen Installation einer globalen, adaptiven Authentifizierung beginnen und dieses Potenzial als Richtlinienverwaltung und Entscheidungspunkt bis auf lokale Ebenen herunterbrechen.

Letztlich lebt Zero Trust aber davon, dass alle Schwachpunkte eines Netzwerks mit Plan identifiziert und beseitigt werden. Schatten-IT, unsichere Betriebssysteme, Unkenntnis der eigenen Angriffsflächen oder mangelnde Verschlüsselung: Viele Baustellen werden bislang auf die leichte Schulter genommen. Das muss sich ändern, wenn man der neuen Generation Hackerangriffe gewappnet sein möchte. Als ersten, pragmatischen Schritt könnten Organisationen mit ihren Management-Konsolen (wie beispielsweise ESET PROTECT) eine Hard- und Software-Inventarisierung vornehmen. Die integrierte Reportfunktion listet auf Knopfdruck Sicherheitsprobleme wie veraltete Betriebssysteme oder ungesicherte Geräte „Endpoint-genau" auf. IT-Teams könnten sich anschließend an die Arbeit machen.

Zum Abschluss drei Tipps aus der Praxis:

1. **Sichtbarkeit:** Identifizieren Sie Geräte und Ressourcen, die überwacht und geschützt werden sollen. Es ist nicht möglich, eine Ressource zu schützen, von der man nichts weiß. Ein Überblick über alle Ressourcen und Zugriffspunkte ist unerlässlich.

2. **Policies:** Richten Sie Kontrollen ein, die nur bestimmten Personen den Zugriff auf bestimmte Ressourcen unter bestimmten Bedingungen erlauben. Mit anderen Worten: Eine granulare Ebene von Richtlinienkontrollen ist erforderlich.

3. **Automatisierung:** Automatisieren Sie Prozesse, um die korrekte Anwendung von Richtlinien sicherzustellen und die Organisation in die Lage zu versetzen, sich schnell an Abweichungen von Standardverfahren anzupassen.

ZUFRIEDENE KUNDEN

Champion Partner

Seit 2019 ein starkes Team auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt

Mehr als 4.000 Postfächer

ISP Security Partner seit 2008

2 Millionen Kunden

BEWÄHRT

Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

Unsere Lösungen sind nach Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystem-übergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

welivesecurity by ESET

Digital Security
Progress. Protected.

ESET.DE | ESET.AT | ESET.CH