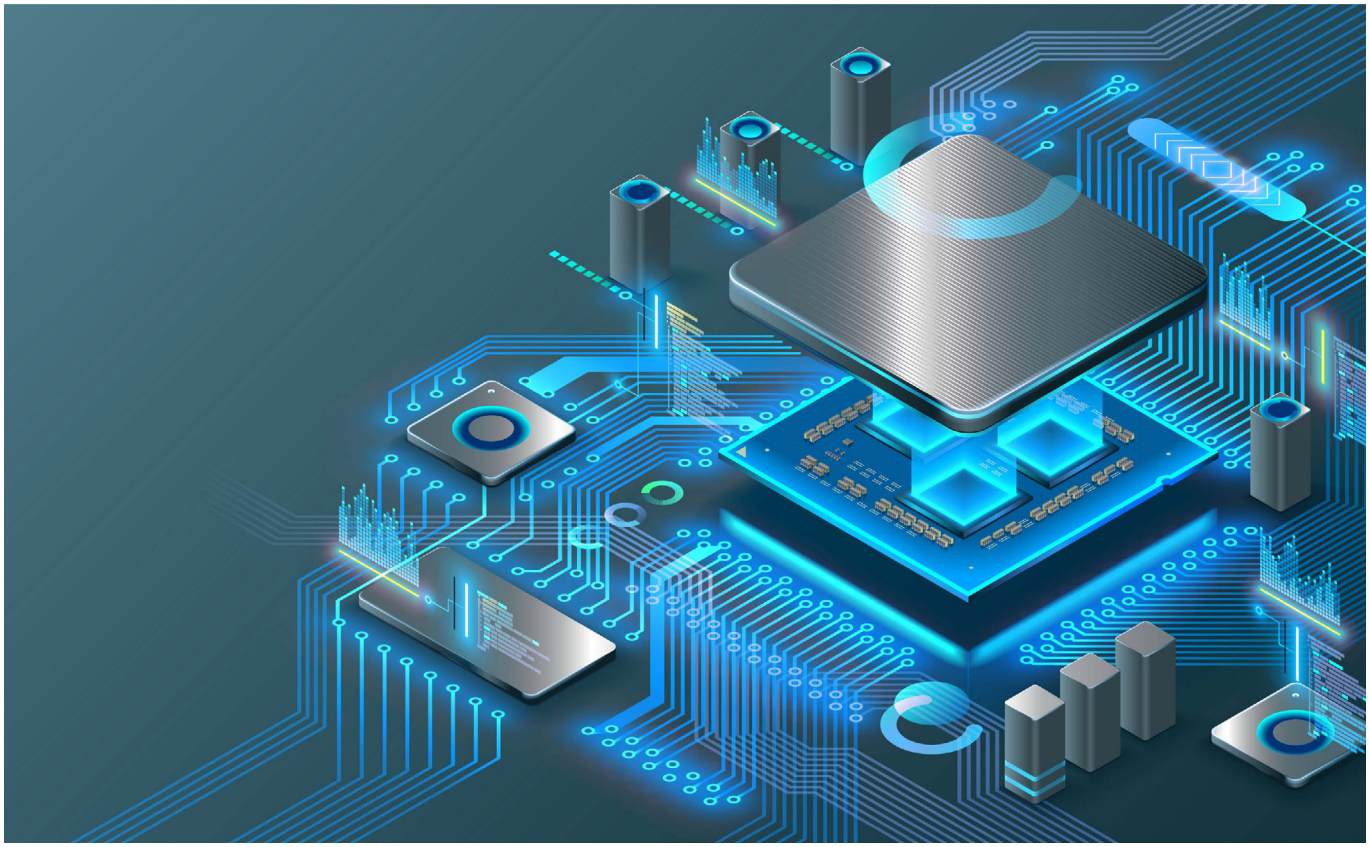


IT-Security:
WARUM DIE UNTERSTÜTZUNG VON ARM-CPUS VIEL MEHR ALS NUR EINE RANDNOTIZ IST

Die jüngsten Statistiken zur IT-Bedrohungslage bei deutschen Unternehmen geben Anlass zur Sorge. Laut Bitkom sehen inzwischen fast zehn Prozent der Unternehmen ihre Existenz durch Cyberangriffe bedroht. Es besteht dringender Handlungsbedarf.

Um sage und schreibe 358 Prozent haben die Schäden durch Cyberangriffe gegenüber 2018/19 zugenommen. Das ist jedenfalls das Ergebnis einer Umfrage bei 1.000 Unternehmen quer durch alle Branchen, die vom Verband Bitkom befragt wurden. In Geld umgerechnet bedeutet das ein Schadensvolumen von gut 220 Milliarden Euro. Daraus leiten sich zwangsläufig zwei Fragen ab. Was sind die Ursachen für eine solche Steigerung und was macht man als Unternehmen dagegen?

Home-Office mit der heißen Nadel gestrickt

Es ist weder abwegig noch falsch, die enorme Zunahme an wirklich schädlichen Cyberattacken mit der Corona-Pandemie in Zusammenhang zu bringen. Denn plötzlich mussten viele Firmen und auch Behörden ihren Betrieb mit zahlreichen Mitarbeitern im Home-Office organisieren, um überhaupt irgendwie überlebensfähig zu sein. Etwas, worauf vielfach weder IT-Verantwortliche noch EDV-Infrastrukturen vorbereitet waren. Und dann hieß die Devise zunächst auch meist: So schnell wie möglich die Betriebsfähigkeit herstellen! Aus der Sicherheitsperspektive ein absolutes Desaster, denn spätestens ab dem Punkt, an dem Firmendaten auf dem Familienrechner bearbeitet wurden und werden, wird erst einmal jegliche Sicherheits-Policy obsolet.

Durch das Home Office wachsen die Anforderungen an IT-Verantwortliche. Auch heterogene Plattform-Strukturen, wo auch ARM-Prozessoren stärker verbreitet sind, erfordern Lösungen

Und das wird auch nur bedingt besser, wenn Mitarbeitende hektisch beschaffte und ebenso hektisch installierte Notebooks an die Hand bekommen. Denn wenn die Geräte denselben, vergleichsweise offenen Router nutzen, über den der Rest der Familie Smartphone-Apps ebenso freimütig verwendet wie sämtliche andere Online-Dienste, tobt womöglich alles an Schädlingen an dem Firmenrechner vorbei, was die IT-Abteilung über Jahre durch Firewalls und Sperren von Diensten versucht hat, aus dem Unternehmens-LAN fernzuhalten. Und man erliegt als Administrator einem Trugschluss, wenn man glaubt, dass eine sichere VPN-Verbindung das Risiko a priori minimiert. Im schlechtesten Fall wandern nämlich auch die Datenpakete der Schadsoftware gut gegen externe Zugriffe geschützt durch den Tunnel. Und verteilt dann noch der Nachwuchs wahlweise aus Versehen oder aus Abenteuerlust wichtige Firmendokumente im Klassenchat, zeigt sich ein weiteres Sicherheitsrisiko von solch improvisierten IT-Lösungen.

Komplexe Anforderungen

Das Ganze ist für IT-Verantwortliche eine immense Herausforderung, beginnend damit, dass der Endpoint-Security zentrale Bedeutung zukommt. Das wiederum wird bei den gerade in der Corona-Zeit entstandenen mitunter inhomogenen Plattform-Strukturen nicht einfacher. Hier hilft die native Unterstützung von ARM-Prozessoren ungemein weiter. Denn nicht nur die neueste Generation der Apple-CPUs – M1 und M2 - setzt auf diese Prozessor-Architektur, auch Microsoft nutzt mit den SQ1- und SQ2 ARM-basierte Zentralrecheneinheiten, weitere Prozessoren sind in Arbeit. Aktuell ist es gerade bei Microsoft im Sinne der Produktivität extrem sinnvoll, dass die Security-Lösungen von ESET ARM nativ unterstützen. Das erspart dem System die Emulation der Erkennungs- und Analyseroutinen auf eine x86-Architektur und die damit verbunden Leistungseinbußen. Denn standardmäßig taktet das Surface Pro X mit SQ2-Chip nur mit 1,8 Ghz. Das ist zwar gut für die Akkulaufzeit, geht aber eben auch zu Lasten der Performance. Und wahrscheinlich möchte sich kein Administrator gerne das chronische Genörgel der Kollegen über zu langsame Rechner anhören. Und die Chefin hat sicherlich auch keine Lust, ständig bei Rückfragen an eine Kollegin oder einen Kollegen häufig „Moment, das lädt noch…“ zu hören.

Allerdings sorgt die Möglichkeit, Erkennungsprozesse in direkter Ansprache der CPU abzuwickeln, nicht nur für geringere Leistungsverluste. Es erhöht mindestens theoretisch auch den Schutz auf den hardware-näheren Layern. Denn es ist durchaus so, dass Rechner auch hardware-seitig vulnerabel sein können. Das NX-Bit bei x86-Prozessoren ist eine Konsequenz auch

diesem Umstand geschuldet? Und auch die Tatsache, dass Windows 11 nur noch auf Systemen installierbar ist, die Secure Boot ermöglichen, trägt der Tatsache Rechnung, dass Schadcode schon lange vor dem Start des eigentlichen Betriebssystems aktiv werden kann. Zwar ist es ein Mythos, dass Hardware selbst durch Viren beschädigt wird, aber zwischen Betriebssystem und den elektronischen Bauteilen steckt eben auch in Festplatten oder Hauptplatinen Programmcode, der dafür sorgt, dass letztlich alle Komponenten als Ganzes funktionieren können.

Trotzdem ist die Endpoint-Security nur ein wichtiger Aspekt und vor allem dann wirksam, wenn sie Teil einer Zero Trust-Strategie ist, die zentral verwaltet wird. Anders ausgedrückt: Der lokale Virenscanner auf dem Mitarbeiter-Rechner ist zwar für den Einzelarbeitsplatz eine Lösung, nicht aber für eine IT-Infrastruktur. Hier erfordert selbst der Grundschutz schon, dass zumindest in gewissem Rahmen eine Firewall den Netzwerkverkehr regelt und eine Sicherheitslösung wenigstens so eklatante Störfaktoren wie Phishing aus dem Netzwerk fernhält. Ganz wichtig ist dabei eine zentrale Verwaltbarkeit. Schließlich kann der Unternehmens-Admin nicht auf den Router des Mitarbeiters im Home-Office zugreifen und sämtliche aus Firmenperspektive unerwünschten Ports blockieren. Auf den Rechner und dessen Sicherheitssoftware dagegen schon, was absolut sinnvoll und nötig ist, damit sich die Unternehmens-Policy zuverlässig umsetzen lässt. Werden dann die Firmendaten noch so abgespeichert, dass auch auf den externen lokalen Systemen die ESET Endpoint Encryption zumindest für diese Daten greift, ist man schon auf einem guten Weg.

Vertraue niemandem

Wirklich sicher wird eine IT-Infrastruktur, wenn man eine Strategie des unbedingten Misstrauens fährt. Vereinfacht gesagt: Die Sicherheitsinfrastruktur geht erst einmal davon aus, dass alles, was von außen in diese Struktur hinein möchte, erst einmal nicht vertrauenswürdig ist (Zero-Trust). Man kann sich das wie eine kontrollierte Pforte an einem Firmeneingang vorstellen. Dabei entbehrt es nicht einer gewissen Ironie, dass manche Unternehmen im analogen Leben sehr viel mehr „Zero-Trust" praktizieren als im digitalen. Stichwort: Mitarbeiterausweis. Sein Vorhandensein sorgt überhaupt erst dafür, dass der Pförtner überhaupt in Erwägung zieht, das Werkstor zu öffnen. Machen wird er es aber im besten Falle erst, wenn er das Foto auf dem Ausweis mit der zugehörigen Person verglichen und für identisch befunden hat. In der IT entspräche das der 2FA, der Zwei-Faktor-Authentifizierung. Dabei kann der erste Faktor durchaus im Verborgenen stattfinden, etwa durch die Maschinen-ID oder physische Adresse der Netzwerkkarte, die so lange als erste Zutrittsstufe funktioniert, wie sie nicht aus dem Netzwerk entfernt wurde. Stufe zwei wäre dann zum Beispiel eine biometrische Authentifizierung mittels Fingerprint oder Gesichtserkennung. Das funktioniert bei einer zentralen Anmeldung etwa im Active Directory. Bei der lokalen Anmeldung sind dann wirklich zwei Schritte nötig, etwa eine Kombination aus Biometrie und Push-Nachricht auf das Smartphone.

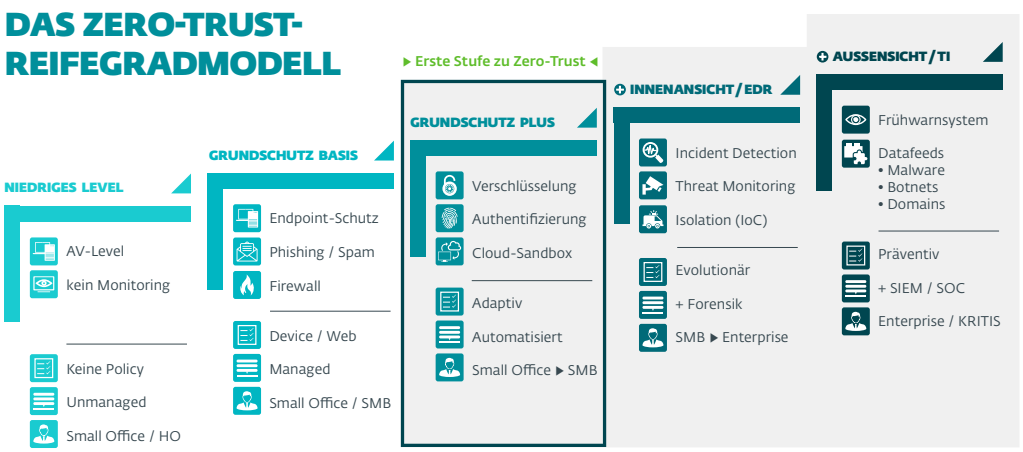
Nun ist es denkbar, dass sich ein betriebsfremder Mensch an der Pforte als Mitarbeiter ausgibt, dem er sehr ähnlich sieht. Und er verschafft sich dadurch Zutritt, weil er sich als bekannt ausgibt. Wäre dieser Mensch, der noch anonyme Hintermänner hat, nun ein IP-Paket, hätte man es hier mit Spoofing zu tun. Besagter Mensch ist dabei der „Mann aus der Mitte" bei diesem „Man-in-the-middle"-Angriff. Eine gute Security-Lösung würde allerdings recht schnell erkennen, dass sich der vermeintliche Mitarbeiter anders verhält als gewohnt und ihn quasi wieder vors Werkstor setzen.

Schwieriger wird es, nachzuvollziehen, was – um in der realen Welt zu bleiben – die Mitarbeiter alles so in ihren Taschen und Rucksäcken hin- und her transportieren, was also die Payload der Datenpakete beinhaltet. Dabei gibt es ganz offensichtlichen Schadcode, dessen Signatur in der Datenbank der Sicherheitssoftware abgelegt ist. Hier sind wir übrigens wieder beim positiven Effekt der nativen Unterstützung vom ARM-Prozessoren. Denn genau dieser permanente Abgleich mit der Signaturdatenbank gehört zu den Prozessen, die dadurch sehr viel effizienter ablaufen.

Manchmal kommt es aber vor, dass die Sicherheitssoftware nicht so genau weiß, wie sie bestimmte Daten bewerten soll. Etwa, wenn letztere bestimmte Merkmale von Schadsoftware aufweisen, die aber eben nicht eindeutig als solche zu erkennen sind. Simpel gestrickte Lösungen verschieben solche Daten einfach in Quarantäne. Ein reiferes Sicherheitskonzept wie der Grundschutz Plus des ESET Zero-Trust-Modells nutzt eine cloudbasierte Sandbox, um eine potenzielle Bedrohung zu identifizieren. Das Ergebnis der Sandbox-Analyse erfahren im Anschluss alle zum Netzwerk gehörigen Geräte, externe inklusive.

All diese bisherigen Sicherheitsmechanismen basieren weitestgehend auf dem Endpoint-Schutz. Damit wird einmal mehr klar, wie wichtig hier eine gute Abstimmung auf die Hardware-Basis ist. Denn logischerweise soll diese komplexe, permanente Selbstkontrolle das System ja möglichst wenig belasten, dabei aber trotzdem jedes mögliche Einfalltor für Schadsoftware – E-Mail, Browser, USB-Sticks etc. –überwachen. Leider sind die Entwickler von ebenjenen Programmen längst keine Hacker mehr, denen es um irgendeinen Proof of Concept geht, auch wenn es die nach wie vor gibt. Aber wie eingangs gezeigt, geht es um viel Geld. Unter anderem durch das Kapern ganzer Firmennetze und das Erpressen von Lösegeld, um die Netze nebst Daten wieder zurückzubekommen. Dabei kann Malware durchaus so entwickelt sein, dass sie gerade große Netzwerke als Cluster nutzt, was die Menge auffälliger Aktivitäten auf den einzelnen Systemen oft bis zur Unkenntlichkeit reduziert. Hier kommt dann ein zentrales Monitoring zum Tragen, das erkennen kann, ob irgendwelche Vorgänge an einer bestimmten Stelle oder in der Summe eine Bedrohung darstellen. Im Idealfall arbeitet so ein Monitoring dabei evolutionär wie der ESET Enterprise Inspector. Das bedeutet, dass das System Erkenntnisgewinne aus Ereignissen in der Vergangenheit zur Bekämpfung gegenwärtiger Bedrohungen und zur Prävention nutzen kann. Hier bewegt man sich dann allerdings von der Skalierung her schon auf dem Enterprise-Level. Das hängt nicht nur mit der Anzahl von Rechnern, Servern und sonstigen zu verwaltenden Komponenten zusammen, sondern auch mit den umfangreichen individuellen Konfigurationsmöglichkeiten, die bei zunehmendem Upscaling des ESET Reifegrad-Modells möglich und nötig sind. Hier muss am Ende das Verhältnis von personellem bzw. Zeitaufwand und Ertrag gewährleistet bleiben.

Mit zunehmender Intensität und Komplexität in Sachen Cyberkriminalität geht auch ein steigender, zumindest virtueller Organisationsgrad der Ausgangssysteme für solche Bedrohungen einher. Es ist, wie schon erwähnt, eben nicht mehr der Hacker im abgedunkelten, verqualmten Hinterzimmer. Vielmehr hat man es hier mit hochprofessionellen EDV-Spezialisten als Teil der organisierten Kriminalität zu tun. Ein kompletter „Wirtschaftszweig“ im Verborgenen sozusagen. Entsprechend konsequent ist es, den Organisationsgrad bei der Bekämpfung solcher Bedrohungen ebenfalls hochzuschrauben, indem man in die Überwachung der eigenen Systeme alle Informationen über die aktuelle globale Bedrohungslage mit einfließen lässt. Das ESET Live Grid ist ein entsprechendes System, dass solche qualifizierten weltweiten Analysen liefert, auf deren Basis präventiv gehandelt werden kann. Und wenn es nur dadurch geschieht, dass man temporär bestimmte Firewall-Ports schließt, weil nur bekannt ist, dass Angriffe darüber erfolgen. Aber Hauptsache, das eigene Netzwerk bleibt davon verschont, auch wenn es dann womöglich für 24 Stunden eingeschränkt nutzbar sein sollte.



Der „Zero Trust Security" Ansatz von ESET besteht aus einem dreistufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung.

Fazit

An dieser Stelle schließt sich der Kreis zur Corona-Pandemie. Da galt und gilt: Es gibt kein Medikament, das das Virus abtötet. Der erste Schritt heißt also, eine Infektion zu verhindern. Und der zweite, mittels Impfung den Organismus möglichst widerstandsfähig werden zu lassen. Genau darum geht es letztlich bei einer umfassenden Sicherheitsstrategie auch. Bekannte Schadroutinen und Angriffsformate löschen und unterbinden, das Eindringen von Bedrohungen möglichst effizient verhindern und, wenn das nicht möglich ist, Systeme so gehärtet zu haben, dass der Schaden minimiert wird. Die Unterstützung einer Hardware-Architektur wie ARM mag dabei auf den ersten Blick ein ganz winziger Baustein sein. Aber wer sich an Zeiten erinnern kann, in denen bei Virenscannern noch vor der Erkennungsrate die Hardware-Auslastung der wichtigste Entscheidungsgrund für oder gegen ein Produkt war, der weiß, wie wichtig es ist, dass eine Sicherheitslösung die Arbeit am Rechner nicht behindern soll. Denn nur dann ist die Produktivität hoch. Nicht nur weil der Rechner flüssig läuft. Sondern auch, weil es deutlich mehr Spaß macht, an einem reibungslos laufenden Rechner zu arbeiten als an einem, an dem bei jedem automatischen Speichern der Cursor einfriert.

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend 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.

ZUFRIEDENE KUNDEN

BVB 09 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

Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

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

CERTIFIED ISO 9001:2015 COMPANY
CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach
Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

200+
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

welivesecurity by ESET