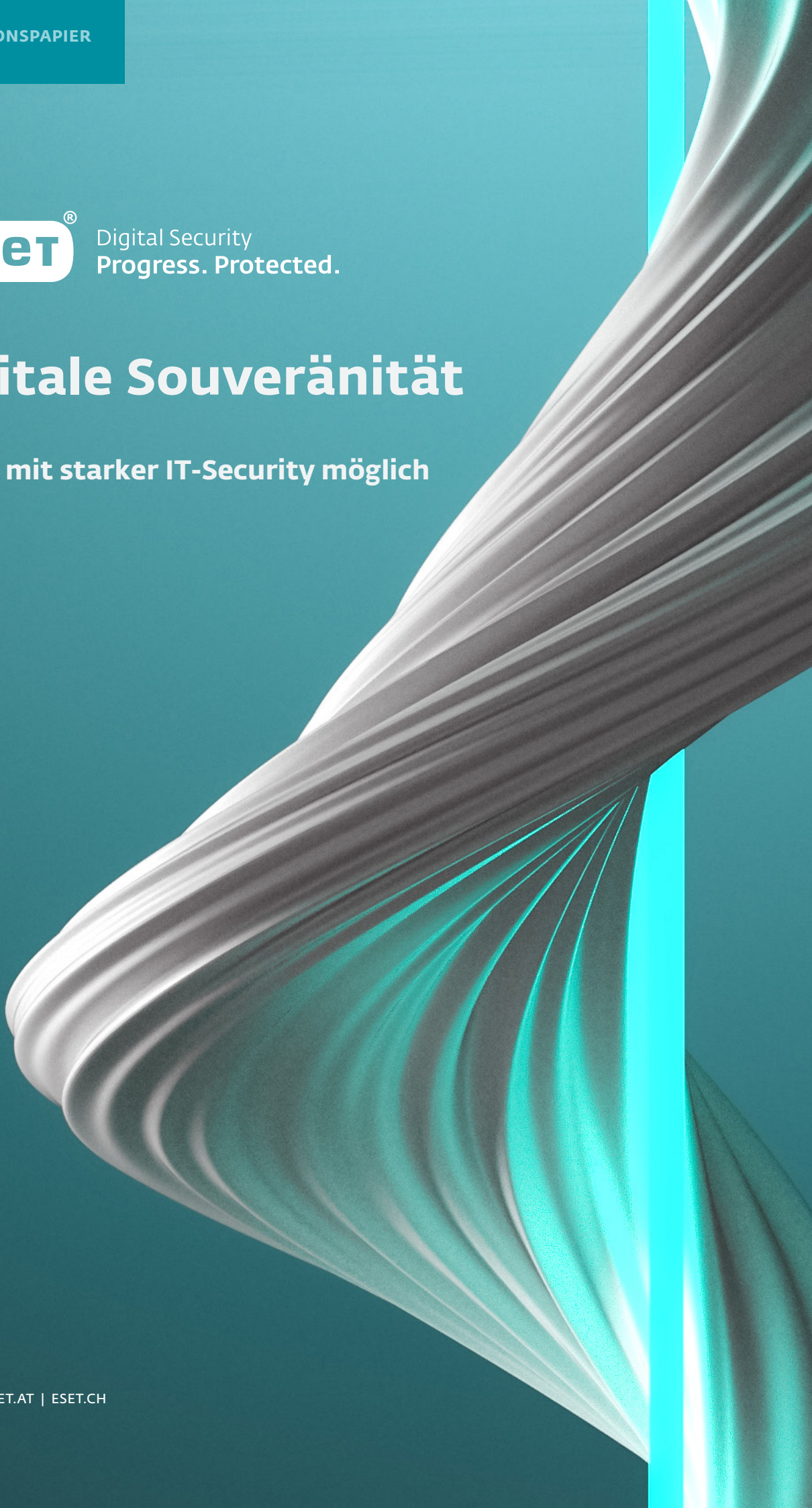
POSITIONSPAPIER

Digital Security
Progress. Protected.

Digitale Souveränität

ist nur mit starker IT-Security möglich



ESET.DE | ESET.AT | ESET.CH

Staatliche Autonomie ist die Voraussetzung dafür, dass Wirtschaft, Gesundheitswesen und unsere Gesellschaft handlungsfähig sind und bleiben. Was einfach klingt, ist heute keinesfalls selbstverständlich. Denn vor allem Versäumnisse im Bereich IT-Security sorgen immer wieder dafür, dass die viel beschworene digitale Souveränität ins Straucheln gerät.

Spätestens seit der Corona-Pandemie wissen wir, dass Europa und insbesondere Deutschland in Bezug auf die digitale Souveränität alles andere als gut dastehen. Mangelhafte oder sogar ganz fehlende Digitalisierungsstrategien offenbarten schon früh in der Pandemie einen enormen Handlungsbedarf. Es zeigte sich schnell, dass Unternehmen, Institutionen und Behörden sich zu stark von Digital-Importen aus dem nicht-europäischen Ausland abhängig gemacht haben, anstatt auf eigene Kompetenzen zu setzen. Die Auswirkungen sind noch immer deutlich spürbar: Lieferengpässe, fehlende Komponenten und Produkte sowie Lösungen, die nicht den europäischen Sicherheitsstandards entsprechen, gehören zu den aktuellen Herausforderungen, an denen Unternehmen und Institutionen zu scheitern drohen. Alles zusammen gefährdet die digitale Souveränität Deutschlands und Europas und könnte langfristig dazu beitragen, dass die wirtschaftliche Stärke auf der Strecke bleibt.

Es fehlt nicht nur an Laptops, Servern oder mobilen digitalen Geräten für die Fernarbeit, sondern auch an Cloud-Infrastrukturen und Anwendungen. Und vor allem mangelt es in vielen Bereichen an ausgereiften IT-Security-Konzepten und Technologien, wie die vermehrten und oftmals erfolgreichen Angriffe auf Behörden, Krankenhäuser und Regierungen gezeigt haben. Dabei ist längst klar, dass digitale Souveränität ohne eine starke IT-Security nicht machbar ist.

IT-Sicherheit als Grundvoraussetzung für ökonomische und politische Selbstbestimmung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt Unternehmen deshalb, 20 Prozent ihres IT-Budgets in Sicherheit zu investieren. Die Realität sieht allerdings anders aus. Nach offiziellen Schätzungen geben Unternehmen aktuell weniger als zehn Prozent ihres gesamten IT-Budgets für technologische Sicherheitsmaßnahmen aus. Hinzu kommt, dass viele Unternehmen auf IT-Security Services aus dem nicht-europäischen Ausland angewiesen sind, wie eine Umfrage des Digitalverbandes Bitkom ergab. Von den 1.100 Organisationen quer durch alle Branchen ab 20 Mitarbeitern waren 55 Prozent davon betroffen. Neun von zehn der befragten Unternehmen sehen die Notwendigkeit, dass Deutschland mehr Geld in IT-Sicherheitslösungen steckt, um sich technologisch besser aufzustellen und der digitalen Souveränität deutlich anzunähern.

Auch für ein souveränes Europa spielt Cybersicherheit eine entscheidende Rolle. Denn digitale Souveränität heißt in erster Linie, eine sichere Dateninfrastruktur für Europa mit geschützten Cyberräumen für Bürgerinnen und Bürger zu schaffen. Das kann nur auf Basis der in Europa geltenden Regeln und Gesetze und nur mit Akteuren aus den eigenen Reihen gelingen. Denn oberstes Ziel der digitalen Souveränität ist es, Manipulation, unberechtigte Zugriffe und Weiterleitung von Daten zuverlässig zu unterbinden.

> *IT-Sicherheit muss bei den EU-Mitgliedsstaaten ganz oben auf der Agenda stehen. Die Bemühungen, eine neue gemeinsame Richtlinie über Netzwerk- und Informationssicherheit zu entwickeln, ist ein richtiger Schritt. Eine umfassende europäische Cybersicherheitsstrategie ist zudem zwingend erforderlich, wenn wir die digitale Souveränität aller EU-Mitgliedstaaten schützen wollen.*
>
> *Thorsten Urbanski, Leiter der TeleTrust-Arbeitsgruppe „IT Security made in EU“*

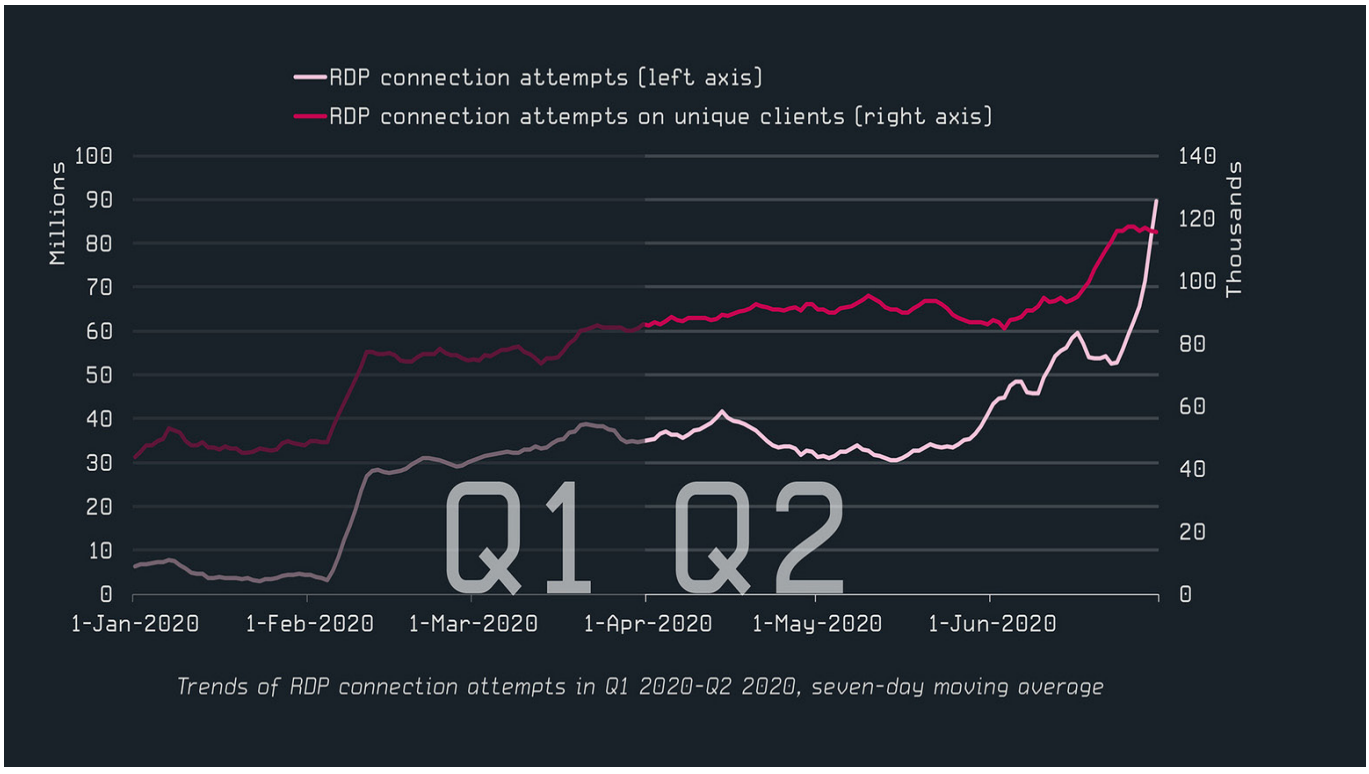
Technologie und Software aus Deutschland und Europa müssen sich deshalb mitsamt verlässlichem IT-Sicherheitskonzept klar positionieren. Nur so lässt sich die Wettbewerbsfähigkeit vorantreiben, gerade auch mit Blick auf Industrie 4.0, aber auch für den Betrieb Kritischer Infrastrukturen (KRITIS). Die verschärfte Bedrohungslage belegt klar, dass insbesondere im Bereich IT-Security umgehender Aufhol- und Handlungsbedarf besteht.

Die Zeit drängt

Cyberkriminelle nehmen Unternehmen, Institutionen und auch Regierungen immer stärker ins Visier. Hacker-Gruppierungen wie LuckyMouse, Winnti Group oder Calypso nutzen dafür selbst kleinste Schwachstellen aus. Ob durch Spionage-, Supply Chain- oder Ransomware-Angriffe – die finanziellen Schäden sind oft immens. Die derzeit größte Bedrohung für staatliche Organisationen geht jedoch klar von sogenannte Advanced Persistent Threats (APTs) aus.

Die erst vor Kurzem bekannt gewordenen Sicherheitslücken in Microsoft Exchange Servern machte E-Mail-Server auf der ganzen Welt zur leichten Beute für Cyberkriminelle. Kleine Firmen gerieten so ebenso ins Visier wie Krankenhäuser, Großkonzerne oder Big Player wie die Europäische Bankenaufsichtsbehörde. Auch Attacken mit Verschlüsselungstrojanern zählen nach wie zu den Angriffsarten, mit denen sich Unternehmen und Institutionen konfrontiert sehen. Jüngstes Beispiel: die Elektronikmärkte von MediaMarkt und Saturn in Deutschland und den Niederlanden. Für Furore sorgte ebenfalls die Ransomware-Attacke auf die US-amerikanische IT-Management-Software Kaseya VSA. Die Kriminellen verlangten ein Lösegeld in Höhe von 70 Millionen US-Dollar.

Auch durch die Verlagerung des Arbeitsplatzes in die heimischen vier Wände öffneten sich zahlreiche „Hintertürchen" für Hacker. So geriet etwa das kostenlose Remote Desktop Protocol unter Dauerbeschuss. Allein im Dezember 2020 registrierte der europäische IT-Sicherheitshersteller ESET in Deutschland, Österreich und der Schweiz täglich durchschnittlich 14,3 Millionen Angriffe. Das entspricht 166 Attacken pro Sekunde.



Trends of RDP connection attempts in Q1 2020-Q2 2020, seven-day moving average

Quelle: ESET Threat Report 2021

IT Security Made in Europe

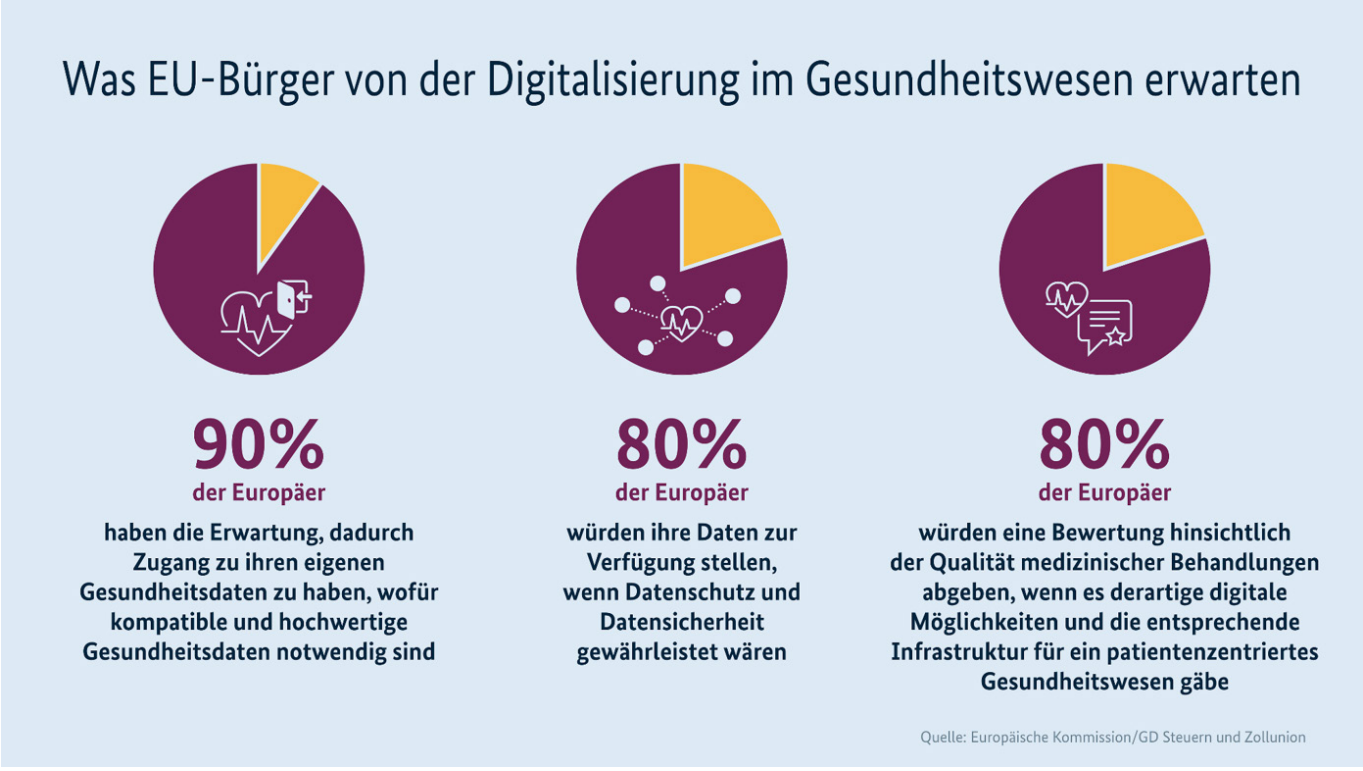
Angriffe wie die Exchange-Attacke sind keine Einzelfälle. Das zeigte beispielsweise die Sicherheitslücke in einer Citrix-Software, über die im September 2020 das Universitätsklinikum Düsseldorf lahmgelegt wurde. Experten gehen davon aus, dass die Bereiche Health und Government im Zuge der fortschreitenden Digitalisierung von Abläufen mit weiteren Angriffen auf Plattformen wie Microsoft SharePoint und Oracle rechnen müssen. Regierungen und Behörden müssen dafür sorgen, dass sie im Bereich Informationssicherheit an Selbständigkeit dazugewinnen, um solchen Bedrohungen zukünftig nicht wehrlos ausgeliefert zu sein.

Wie wichtig das ist, zeigt eine Befragung der Europäischen Kommission. Demnach würden 80 Prozent der Europäer ihre Gesundheitsdaten zur Verfügung stellen würden, wenn Datenschutz und -sicherheit gewährleistet sind. Dieser Fall und andere Beispiele belegen, wie essenziell das Vertrauen in Informationsschutz und Datensicherheit ist, um die Digitalisierung in Deutschland und in Europa voranzubringen.

Aus diesem Grund hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) die optionale Kennzeichnungsmöglichkeit „IT Security made in EU" (ITSMIE) ins Leben gerufen. Mit diesem Vertrauenssiegel können sich europäische Hersteller von IT-Security-Lösungen von ausländischen Mitbewerbern abheben und zeigen, dass ihre Lösungen den strengen europäischen Datenschutzbestimmungen entsprechen. Das Siegel soll nicht nur Vertrauen signalisieren, sondern Produkte und Technologien aus der EU in den Fokus von Wirtschaft und Government bringen.

So können beispielsweise Behörden bei Ausschreibungen davon ausgehen, dass eine mit dem Siegel „IT Security made in EU" ausgezeichnete Lösung höchsten Anforderungen genügt.

Organisationen und Anwender stellen damit sicher, dass sie auf die Leistungsfähigkeit und Zuverlässigkeit der gekennzeichneten Technologien und Lösungen ebenso vertrauen können wie auf deren bedingungslose Gesetzeskonformität. Denn mit diesem Siegel verpflichten sich Hersteller mit Hauptsitz in der EU freiwillig dazu, dass ihre Security-Lösungen vertrauenswürdig sind, strengsten Datenschutzauflagen entsprechen und keinerlei versteckte Backdoors enthalten: Das Unternehmen muss sich verpflichten, die Anforderungen der EU-Datenschutz-Grundverordnung abzudecken.



Quelle: Europäische Kommision/GD Steuern und Zollunion

- Der Unternehmenshauptsitz muss in der EU sein.
- Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
- Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (keine „Backdoors“).
- Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in der Europäischen Union stattfinden.
- Das Unternehmen muss sich verpflichten, den Anforderungen der EU-Datenschutz-Grundverordnung zu genügen.

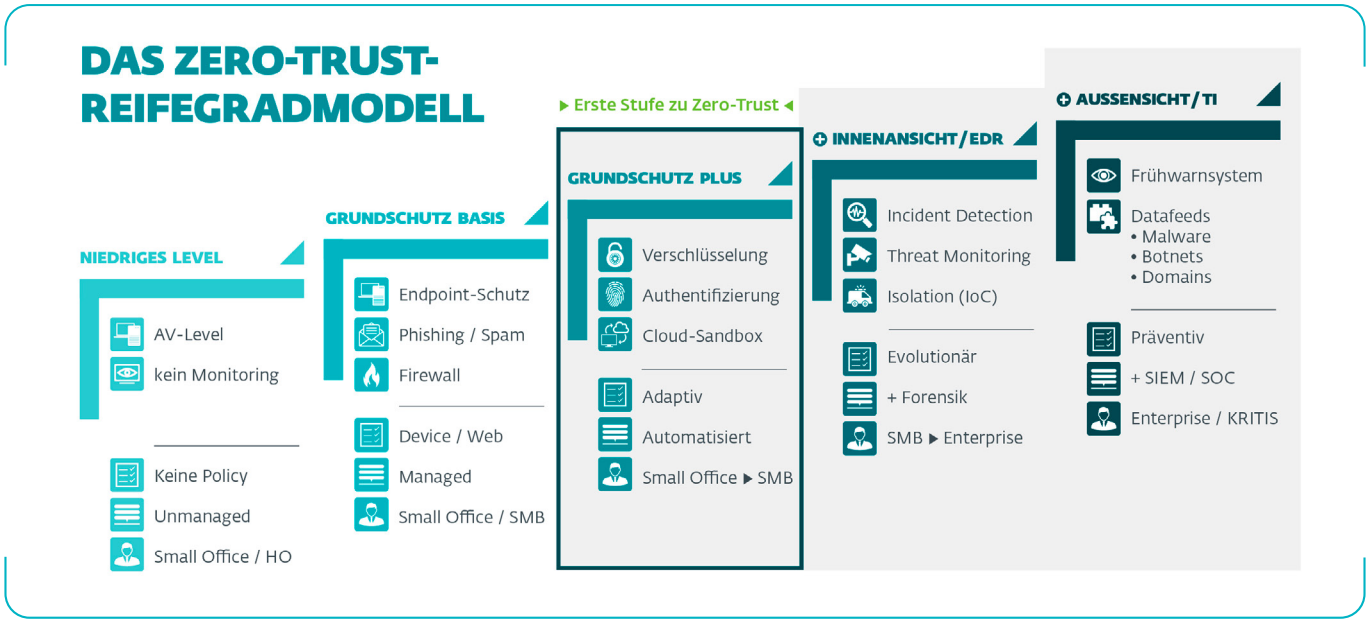
ESET: Die europäische Antwort auf Cybercrime

100 Unternehmen haben sich der Initiative bereits angeschlossen. Als eines der ersten Unternehmen war der IT-Security-Hersteller ESET mit dabei. Mit Unterzeichnung der freiwilligen Konformitätserklärung hat ESET sein Engagement im Bereich EU-Datenschutz und vertrauenswürdige IT-Schutzlösungen besiegelt. Darüber hinaus hat der Security-Spezialist in den Jahren 2020 und 2021 mehrere Forschungskooperationen gestartet, unter anderem mit der Europäischen Organisation für Kernforschung (CERN), Europol und der französischen Nationalen Agentur für Sicherheit der Informationssysteme (ANSSI). Auch in Zukunft soll es weiteren Austausch mit transnationalen Cyber-Security-Organisationen geben.

Vorausschauendes Denken und Handeln ist auch genau das, was Organisationen im Kampf gegen Cyberkriminelle dringend brauchen. Bei den Microsoft Exchange Angriffen wären viele Behörden und Unternehmen durch den Einsatz von Endpoint Detection und Response Lösungen verschont geblieben. Diese Technologie sucht pausenlos im eigenen System nach Sicherheitslücken, verdächtigem Verhalten und ungewöhnlichen Ereignissen.

Damit Organisationen Angriffe von außen, Fehlverhalten von Mitarbeitern und unerwünschte Anwendungen schnellstmöglich identifizieren können, müssen sie umfassend über die Vorgänge in ihrem Netzwerk informiert sein. Wie die ESET-Forscher ermittelt haben, geraten Organisationen vor allem aus drei Gründen zunehmend ins Visier von Kriminellen:

- Technische Unzulänglichkeit bedingt durch die Corona-Pandemie
- Ungeschulte Mitarbeiter werden ungewollt zu Security-Schwachstellen
- Der Aufstieg von Cyberkriminellen zu Profi-Hacker-Gruppen



Das ESET Reifegradmodell zeigt, was für die Umsetzung des „Zero Trust Security“-Konzepts wichtig ist.

Sicherheit aus einem Guss: Zero Trust als Strategie

Zweifellos müssen sich Behörden und Unternehmen der Herausforderung Digitalisierung stellen. Wenn IT-Verantwortliche proaktiv handeln wollen, sollten sie in ihrer Organisation einen konsequenten Zero-Trust-Security-Ansatz verfolgen. Denn die konventionellen Schutzlösungen, bestehend aus Malware- und Spamfilter sowie Firewall, reichen heute längst nicht mehr aus, um Cyberattacken zuverlässig abzuwehren. Professionelle APT-Angriffe umgehen immer häufiger diese Mechanismen, indem sie schleichend, unbemerkt und mehrstufig die Systeme infiltrieren. Aus diesem Grund hat ESET den Zero-Trust-Ansatz entwickelt und an die Anforderungen unterschiedlicher Organisationsgrößen angepasst. Bei Zero-Trust werden alle internen und externen Geräte, Prozesse und Personen zunächst einmal als potenziell gefährlich eingestuft, um keinerlei Risiko einzugehen. Mit dem vollumfänglichen Schutz aller Geräte von innen und außen geht ESET sogar einen Schritt weiter, als es das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert.

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 Endpoints" folgt. Sie eignet sich unabhängig vom individuellen Schutzbedarf für jede Organisationsgröße. Dank der hohen Flexibilität ist er zudem branchenbergreifend problemlos auf die Bedürfnisse der Unternehmen, Behörden oder die des Gesundheitswesens anwendbar. Daran schließen sich zwei Zero Trust-Stufen mit weiter steigenden Security-Maßnahmen und -Diensten an.

ESET entwickelt alle Technologien in Eigenregie und in den eigenen Forschungslabors. Dazu zählen auch Multi-Faktor-Authentifizierung und Datenverschlüsselung - und das über alle gängigen Betriebssysteme hinweg, cloudbasiert oder On-Premises. Dadurch sind die ESET-Sicherheitslösungen aus einem Guss und basieren dem Bekenntnis zu „Zero Trust Security". Ein gutes Beispiel dafür, wie zukunftsfähige IT-Security-Lösungen aussehen müssen, damit sie für Unternehmen, Institutionen und Behörden zum sicheren Anker ihrer digitalen Souveränität und damit zur Investition in die Zukunft Europas werden.

Autoren:

Thorsten Urbanski und Ildiko Bruhns, *ESET Deutschland GmbH*

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 Endpoint Detection and Response Lösungen und Frühwarnsysteme wie Threat Intelligence Services ergänzen das Angebot im Hinblick auf Forensik sowie gezieltem Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Repudationsdatenbank 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

T

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Security 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.
Nutzer weltweit

400k+
Business-Kunden

200+
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

welivesecurity by ESET


Digital Security
Progress. Protected.
ESET.DE | ESET.AT | ESET.CH