PAPER

Ransomware 2025: Wenn Daten zum Druckmittel werden

Wie sich Unternehmen vor der gefährlichen Erpressersoftware schützen

Cybersecurity
Progress. Protected.

Vorwort

Ransomware bleibt auch 2025 eine der größten Bedrohungen für Unternehmen. Sie entwickelt sich ständig weiter, zeigt eine noch nie dagewesene Raffinesse und verursacht hohe Schäden. Laut der jüngsten Studie des Digitalverbands Bitkom haben 2024 ein Drittel der deutschen Unternehmen durch erpresserische Software einen Schaden erlitten.

Eine andere Umfrage des ↗Ponemon Institute unter mehr als 500 deutschen Firmen ergab sogar, dass 89 Prozent der Befragten von einem Ransomware-Angriff betroffen waren. Allerdings wird nicht deutlich, ob erfolgreiche Attacken oder auch gescheiterte Versuche hier reinzählen. Klar wird nur eines: Ransomware-Angriffe bedeuten für Unternehmen viel Aufwand, Betriebsausfälle und massive Kosten. Mehr als die Hälfte hatten nach einer Attacke mit Geschäftsunterbrechungen zu kämpfen, 1,4 Millionen US-Dollar betrug das durchschnittliche Lösegeld und nur jeder zehnten Firma gelang die Rekonstruktion ihrer Daten. Knapp die Hälfte der Unternehmen musste schmerzhafte Umsatzeinbußen hinnehmen und ein Drittel verlor neben den Daten auch ihre Reputation, deren Wiederherstellung sich als größter Kostenfaktor von allen erwies.

Ransomware-Angriffe sind heute professioneller, systematischer und schlagkräftiger denn je. Die Erpressersoftware hat sich zu einem der lukrativsten Geschäftsmodelle für Cyberkriminelle gemausert. Die Ziele der Hacker bleiben nach wie vor unverändert: Schnelles Geld und die strategische Schädigung von Unternehmen, Infrastrukturen und sogar ganzen Staaten. Erschwerend hinzu kommen neue Techniken und Werkzeuge wie die gefürchteten „EDR-Killer". Diese Malware hat es auf Endpoint Detection and Response-Lösungen (EDR) abgesehen und schaltet sie gezielt aus, um den Weg für nachfolgende Ransomware-Angriffe zu ebnen. Ein Beispiel ist hierfür der „EDRKillShifter", der von der Hackergruppe RansomHub entwickelt wurde. Er nutzt Schwachstellen in legitimen Treibern aus, um Sicherheitslösungen zu umgehen.

Diese Entwicklungen zeigen: Reaktive Maßnahmen reichen schon lange nicht mehr aus. Vielmehr müssen Unternehmen eine Cybersicherheitsstrategie verfolgen, bei der Prävention im Vordergrund steht.

Mit diesem Whitepaper klären unsere ESET Experten Unternehmen branchenübergreifend über die Gefahren von Ransomware auf und zeigen die neuesten Trends in dem Bereich. Im ersten Teil beleuchten sie neue Entwicklungen und Werkzeuge in der Ransomware-Szene. Der zweite Teil richtet sich an Entscheidungsträger und liefert ihnen nützliche Tipps, wie sie ihre Organisation gegen die Erpressersoftware schützen und worauf sie dabei achten sollten.

Inhaltsverzeichnis

Cybersecurity
Progress. Protected.

RANSOMWARE: TRENDS, TOOLS & TAKTIKEN

Ransomware kostet Organisationen Milliarden an Euro

Unternehmen jeder Größe und Branche sehen sich seit Jahren Cyberangriffen ausgesetzt. Im Jahr 2024 belief sich der Gesamtschaden durch analoge und digitale Cyberkriminalität in Deutschland auf über 266 Milliarden Euro, davon 178,6 Milliarden Euro durch Cybercrime, so der ↗Bitkom-Verband. Das sind rund 30 Milliarden Euro mehr als im Vorjahr. Fast ein Drittel und damit der größte Schaden ist auf Ransomware zurückzuführen.

Doch die Aussicht auf schnelles Geld ist nicht der einzige Anreiz für Erpressersoftware. Viele Hackergruppen, allen voran die staatlich geförderten, verfolgen auch taktische und strategische Ziele. Advanced Persistent Threats (APT)-Gruppen setzen Ransomware ein, um Spuren früherer Aktivitäten in Unternehmensnetzwerken zu verwischen. Die Malware wird auch genutzt, um kritische Infrastrukturen zu stören. Damit ihre Attacken erfolgreich sind, nutzen die Angreifer verschiedene Wege: Schwachstellen in der Lieferkette, Zero-Day-Exploits und KI-gestütztes Phishing, was die Reichweite und Wirkung von Ransomware-Angriffen maximiert.

60%

der deutschen Unternehmen wurden bereits mit Ransomware ↗angegriffen

Neues aus der professionellen Erpresserszene

Seit 2024 gibt es einige frische Trends bei Ransomware und massive Weiterentwicklungen. Sie geben uns einen ersten Vorgeschmack, womit wir in den nächsten Jahren rechnen könnten.

Eines der sicherlich wichtigsten Ereignisse war Anfang 2024 die Zerschlagung der Ransomware-as-a-Service (RaaS)-Gruppe Lockbit. Auf ihr Konto ging die weltweit am häufigsten eingesetzte, namensgleiche Erpressersoftware. Doch wo immer ein großer Player verschwindet, entsteht ein Machtvakuum, das sich schnell wieder füllt. Neue Hackergruppen nutzten die Gelegenheit, um den Platz von Lockbit einzunehmen. Die berühmt-berüchtigten Bedrohungsakteure von RansomHub machten am Ende das Rennen, die sich mit Angriffen auf die unterschiedlichsten Branchen schon einen Namen gemacht hatten: Regierungsdienste und -einrichtungen, Transportwesen, Gesundheitssektor oder Landwirtschaft. RansomHub war allein im ersten Halbjahr 2025 für 500 erfolgreiche Cyberattacken verantwortlich.

Was ist RaaS?

Ransomware-as-a-Service (RaaS) ist ein illegales Geschäftsmodell, bei dem professionelle Hackergruppen ihre Erpressersoftware anderen Kriminellen („Affiliates") gegen „Umsatzbeteiligung" zur Verfügung stellen – ähnlich wie bei legitimen SaaS-Plattformen (Software-as-a-Service). Zu den Vorteilen für Cyberkriminelle gehören:

- Geringe Einstiegshürde für Kriminelle (Plug-and-Play)
- Professionelle Partnerprogramme (z. B. 90 % Umsatzbeteiligung bei RansomHub)
- Permanente Weiterentwicklung von Taktiken und Angriffswerkzeugen
- Verlagerung des Risikos auf die ausführenden Akteure

So funktioniert das Modell:

Rolle	Aufgabe
RaaS-Entwickler	Entwicklung und Pflege der Ransomware-Plattform (inkl. Support und Dashboard)
Affiliates	Ausführende Akteure der eigentlichen Angriffe (Phishing, Initial Access etc.)
Opfer	Unternehmen oder Privatpersonen, deren Daten verschlüsselt werden
Zahlungsabwicklung	Meist über Kryptowährungen – Anonymität spielt zentrale Rolle
Provisionierung	Affiliates erhalten einen Teil der Lösegeldsumme

Auf der Suche nach neuen Partnern

RaaS- und andere Hackergruppen stehen vor ähnlichen Herausforderungen wie legitime Unternehmen. Die Konkurrenz ist groß und es braucht unternehmerisches Geschick, um sich von Mitbewerbern abzuheben. Aus diesem Grund entwickeln und aktualisieren Cyberkriminelle ihre eigenen Partnerprogramme, um neue Geschäftspartner zu gewinnen. RansomHub lockt „Rekruten" mit einem interessanten Angebot: Hacker, die die Malware der Gruppe einsetzen, dürfen 90 Prozent des erbeuteten Lösegelds behalten. Die restlichen 10 Prozent beansprucht RansomHub für sich, allerdings auf Vertrauensbasis, denn einen Kontrollmechanismus für Zahlungen gibt es nicht. Das heißt, die Kriminellen müssen auf die „Ehrlichkeit" ihrer Partner bauen. So gelingt es diesen aufsteigenden Kriminellen, zahlreiche neue Partner zu gewinnen, die zuvor mit anderen RaaS-Anbietern wie LockBit und BlackCat zusammengearbeitet haben.

Neue berühmt-berüchtigte Hackergruppen

Es ist schwierig, RaaS-Anbieter und ihre Methoden vollständig zu verstehen, ohne die Advanced Persistent Threat (APT)-Gruppen zu berücksichtigen. Diese Allianzen aus Bedrohungsakteuren nutzen Erpressersoftware nicht nur für finanzielle Gewinne, sondern verfolgen auch weitreichende strategische Ziele. Die folgenden APT-Gruppen waren in letzter Zeit vermehrt an Ransomware-Angriffen beteiligt:

Gruppe	Verbindung nach	Ziele	Taktiken & Tools
ChamelGang	China	Regierung, Infrastruktur	Tarnung durch Ransomware, CatB-Malware
Moonstone Sleet	Nordkorea	Technologie, Finanzen	Fake-Firmen, trojanisierte Spiele, FakePenny-Malware
Pioneer Kitten	Iran	Verteidigung, Bildung	Initial Access Broker
Andariel	Nordkorea	Gesundheitssektor USA	Teil der Lazarus-Gruppe, Ransomware

EDR-Killer ist der neueste Trend

Nicht nur die Vertriebsmethoden der RaaS-Anbieter entwickeln sich weiter. Hacker setzen auch immer raffiniertere Techniken ein, um eine frühzeitige Erkennung zu verhindern oder die Verbreitung im Unternehmensnetzwerk zu beschleunigen. Dazu zählen die zu Beginn erwähnten EDR-Killer, die bei Ransomware-Banden sehr beliebt sind. Sie sollen die Endpoint Detection and Response (EDR)-Lösungen deaktivieren, damit nachgeladene Malware nicht erkannt wird.

Einige Cyberkriminelle entwickeln inzwischen maßgeschneiderte EDR-Killer für bestimmte Lösungen und bieten sie als Teil ihrer RaaS-Programme an. Gleichzeitig erstellen sie ihre Verschlüsselungs-Malware in weit verbreiteten Programmiersprachen wie Rust und Go. So können sie möglichst viele Systeme plattformübergreifend infizieren.

Was sind EDR-Killer?

EDR-Killer sind spezialisierte Schadprogramme, die Sicherheitslösungen deaktivieren, indem sie Techniken wie „Bring-your-own-vulnerable-driver" (BYOVD) ausnutzen. Dabei installieren Angreifer zunächst legitime, aber anfällige Gerätetreiber und nutzen deren Schwachstellen dann aus, um privilegierte Aktionen aus dem Kernel-Bereich auszuführen. Dadurch können sie Sicherheitskontrollen umgehen, Sicherheitsprozesse beenden und Erkennungs- und Schutzmechanismen ausschalten.

EDR-Killer haben sich zu einem festen Bestandteil von Ransomware-Angriffen entwickelt. Unsere ESET Experten gehen davon aus, dass Cyberkriminelle diese Werkzeuge im Jahr 2025 weiter verfeinern, wodurch sie immer ausgefeilter werden und so schwerer zu erkennen sind. Gleichzeitig zeigt dieser Trend, dass Cyberkriminellen Sicherheitstools wie EDR ein Dorn im Auge sind: Sie schaffen es, Hacker von Unternehmenswerten fernzuhalten und werden deshalb gezielt angegriffen.

Ransomware kann jeden treffen – auch Endnutzer

In der Praxis sind nicht nur Unternehmen und Organisationen Ziel von Ransomware-Angriffen. Bedrohungsakteure richten sich zunehmend auch systematisch gegen Privatnutzer. Im August 2024 starteten Cyberkriminelle eine groß angelegte weltweite Ransomware-Kampagne, die gezielt Geräte von Endanwendern verschlüsselte. Der Grund dafür ist einfach: Privatnutzern fehlt es häufig an angemessener IT-Sicherheitssoftware und Erfahrung mit Cyberkriminalität. Die Verbreitung der Erpressersoftware ↗Magniber erfolgte über schadhafte Software-Downloads, gefälschte Updates und Key-Generatoren. Für die Entschlüsselung forderten die Erpresser Lösegelder zwischen 1.000 und 5.000 US-Dollar. Für ihre Angriffe nutzte die Schadsoftware Zero-Day-Lücken in Windows, gefälschte Windows- und Browser-Updates sowie trojanisierte Software-Cracks.

Deshalb gilt: Auch im Privatleben sollten Nutzer auf der Hut vor cyberkriminellen Aktivitäten sein. Vorbeugende Maßnahmen wie eine gesunde Grundskepsis und eine moderne, topaktuelle IT-Sicherheitslösung reduzieren das Risiko, Opfer eines Ransomware-Angriffs zu werden.

Warum es sich niemals lohnt, Lösegeld zu zahlen

Der Grundsatz „Das Beste hoffen und mit dem Schlimmsten rechnen" erweist sich auch in der digitalen Welt angesichts der Erfolgsquote von Ransomware-Attacken großer Beliebtheit. Selbst mit dem besten Präventionsansatz ist ein Angriff mit Erpressersoftware möglich. Was also tun, wenn die eigenen Daten verschlüsselt wurden und ein fieser Erpresserbrief auf dem Bildschirm erscheint?

In Kurzfassung:
Zahlen Sie niemals Lösegeld!

Die lange Antwort lautet: Unternehmen, die schnell handeln, auf Notfallpläne zurückgreifen und auf sichere Backups setzen, können sich erholen, ohne sich auf die Erpressung einlassen zu müssen.

Bezahlen Sie allerdings die Kriminellen, die Ihre Daten verschlüsselt haben, bedeutet das:

- Sie bestätigen das Geschäftsmodell hinter der Straftat.
- Sie fördern weitere kriminelle Aktivitäten, indem Sie diese mitfinanzieren. Außerdem ermöglichen Sie es Ransomware-Banden, Zero-Day-Schwachstellen zu erforschen und neue Exploits zu entwickeln
- Sie stehen nun auf der Liste zahlbereiter Opfer und werden höchstwahrscheinlich Ziel zukünftiger Ransomware-Angriffe und weiterer Geldforderungen sein.

Die Zahlung des Lösegelds ist darüber hinaus keine Garantie dafür, dass Cyberkriminelle einen funktionierenden Entschlüsselungscode bereitstellen. Letztlich gibt es keine Möglichkeit, sie zur Rechenschaft zu ziehen oder rechtliche Schritte gegen sie einzuleiten.

Jedes
8.
Unternehmen
in Deutschland hat bereits Lösegeld ↗gezahlt

Es gibt mehrere Gründe, weswegen eine Zahlung möglicherweise nicht zur Wiederherstellung der Daten führt:

- Einige Daten könnten während der Verschlüsselung beschädigt worden sein, sodass sie nicht rekonstruiert werden können.
- Das zur Verfügung gestellte Entschlüsselungstool kann mit zusätzlicher Malware oder Fehlfunktionen behaftet oder deutlich langsamer als die Wiederherstellung aus Backups sein.
- Der Entschlüsselungsprozess selbst kann scheitern, z. B. aufgrund von Fehlern im Entschlüsselungsschlüssel, einem zu komplizierten Verschlüsselungsschema oder Komplikationen bei der Zahlungsabwicklung (insbesondere bei Kryptowährungen).
- Der Angreifer handelt schlicht böswillig, ohne die Absicht, einen Entschlüsselungsschlüssel zur Verfügung zu stellen.

BYE, BYE RANSOMWARE: MODERNE TECHNOLOGIEN & MASSNAHMEN GEGEN RANSOMWARE

Ransomware ist häufig die letzte Phase eines Angriffs, der mit anderen Bedrohungen wie Phishing, Exploits, Brute-Force-Angriffen, gestohlenen Zugangsdaten, Downloadern oder maßgeschneiderter Schadsoftware startet. Mit Ransomware versuchen Cyberkriminelle gezielt, am Ende der „Malware-Kette" noch das letzte bisschen Geld aus der betroffenen Organisation herauszupressen.

Ein mehrschichtiger Sicherheitsansatz befähigt Organisationen, sich vor solchen Attacken zu schützen. Die Automatisierung der Schutzmechanismen hilft, schnell auf Angriffe zu reagieren, bevor größerer Schaden entsteht. Eine präventive Strategie blockiert Cyberangriffe schon im Vorfeld, indem sie jede Phase eines Angriffszyklus abdeckt. Viele Organisationen haben das Potenzial eines „Prevention First"-Ansatzes bereits erkannt, der u. a. folgende Maßnahmen umfasst:

Mitarbeiterschulungen

Phishing bleibt nach wie vor eine der Hauptursachen für Ransomware-Angriffe. Dieser Verbreitungsweg für Erpressersoftware ist deswegen so erfolgreich, weil Mitarbeitende häufig die typischen Anzeichen dieser Betrugsversuche nicht (er-)kennen, auf unbekannte Links klicken oder unwissentlich Anhänge herunterladen.

Mit regelmäßigen Schulungen für die Identifizierung gefälschter E-Mails und Webseiten, der Erstellung wie Verwendung sicherer Passwörter und Nutzung einer Multi-Faktor-Authentifizierung lassen sich die Angriffsrisiken erheblich reduzieren. Wird eine EDR-Lösung eingesetzt, ist es darüber hinaus wichtig, dass IT-Mitarbeitende deren Vorteile und Funktionsweise verstehen, denn damit können schädliche Aktivitäten im Unternehmensnetzwerk frühzeitig erkannt und blockiert werden.

Netzwerksicherheit und Patch-Management

Diese proaktiven Abwehrstrategien tragen dazu bei, eine robuste Cybersicherheit herzustellen. In der IT-Sicherheit lautet das Motto: Vorbeugen ist immer besser als heilen. Weitere wichtige Schritte einer präventiven Sicherheitsstrategie sind der Einsatz von Netzwerksicherheitsmaßnahmen wie Firewalls, Intrusion Detection Systeme (IDS) und eine Netzwerksegmentierung. Sie helfen, den Datenverkehr zu kontrollieren und zu überwachen, unberechtigte Zugriffe zu verhindern und die Verbreitung von Ransomware einzudämmen.

Kaum eine dieser Maßnahmen lässt sich ohne regelmäßiges Patch-Management umsetzen. Es stellt sicher, dass alle Systeme und Anwendungen auf dem neuesten Stand sind und es keine Schwachstellen gibt, die Angreifer ausnutzen könnten.

Zero Trust als Sicherheitsstandard

Hinter Zero Trust steht die Idee der konzeptionellen Leitlinie „Vertraue nie, überprüfe immer", die auf Vorsicht und Skepsis sowohl intern als auch extern eines Unternehmens beruht. Das Zero Trust-Modell baut die Sicherheit um die wichtigsten Ressourcen und Entitäten einer Organisation herum auf: Daten, Netzwerke, Geräte, Workloads und Personen. Heute gehört diese Architektur zum Standardbereich der Cybersicherheit, weil damit das Risiko eines unbefugten Zugriffs weiter eingedämmt wird.

Datensicherung und Wiederherstellbarkeit

Der Schutz kritischer Daten ist ebenfalls ein entscheidender Faktor für einen präventiven Sicherheitsansatz. Informationen, die offline oder in sicheren Cloud-Umgebungen gespeichert werden, sind für die Wiederherstellung nach einem Angriff unerlässlich. Diese Backups sollten regelmäßig getestet werden, um ihre Wirksamkeit zu garantieren.

Schutz vor Phishing und E-Mail-Angriffen

Im täglichen Betrieb helfen präventive E-Mail-Sicherheitsmaßnahmen wie Filter und Spam-Schutz, um schädliche E-Mails und Anhänge zu blockieren, bevor sie die Nutzer erreichen.

Viele Vorfälle sind auf menschliches Versagen zurückzuführen, wobei E-Mails nach wie vor ein beliebtes Einfallstor sind.

Reaktionsfähigkeit im Ernstfall

Ein gut ausgearbeiteter Incident Response Plan (Notfallplan) und regelmäßige Übungen stellen sicher, dass Organisationen effektiv auf Ransomware-Angriffe reagieren können.

So hilft ESET bei der Abwehr und Wiederherstellung nach Ransomware-Angriffen

ESET bietet Unternehmen einen umfassenden Schutz vor Ransomware durch eine Kombination aus proaktiven Erkennungstechnologien, mehrschichtigen Sicherheitsfunktionen und effektiven Wiederherstellungsmechanismen.

Ransomware Shield

#1 Das Ransomware Shield ist eine Sicherheitsfunktion, die als Teil des Host-based Intrusion Prevention Systems (HIPS) in den Endpoint-Lösungen von ESET integriert ist. Sie überwacht und blockiert automatisch Anwendungen, die sich wie Ransomware verhalten. Administratoren können diese Funktion über die Web-Konsole ESET PROTECT konfigurieren, indem sie den Schutz aktivieren oder den Audit-Modus einschalten. In letzterem Vorgang werden erkannte Bedrohungen gemeldet, aber nicht automatisch blockiert. Dies ermöglicht, Fehlalarme zu identifizieren und legitime Anwendungen auszuschließen.

Ransomware Remediation

#2 Diese Technologie ergänzt das Ransomware Shield, indem sie eine automatische, geschützte Notfall-Backup-Funktion bereitstellt. Sobald verdächtiges Verhalten erkannt wird, erstellt ESET Ransomware Remediation in Echtzeit gesicherte Dateiversionen in einem geschützten Bereich. Wenn eine Ransomware-Infektion bestätigt wird, stellt die Technologie die betroffenen Dateien sofort wieder her. Ein wesentlicher Vorteil ist, dass diese Backups vor Angriffen geschützt sind und nicht von der Ransomware selbst gelöscht oder verschlüsselt werden können.

Erweiterte HIPS-Regeln

#3 Zusätzlich zum standardmäßigen Ransomware Shield können Administratoren spezifische HIPS-Regeln konfigurieren, um den Schutz weiter zu verstärken. Beispielsweise können Regeln erstellt werden, die das Starten von Prozessen durch bestimmte Anwendungen wie wscript.exe, cscript.exe oder powershell.exe verhindern. Diese Maßnahmen erschweren es Ransomware, sich im System auszubreiten oder zusätzliche Schadsoftware nachzuladen.

Mehrschichtige Schutztechnologien

#4
- **Advanced Memory Scanner:** Überwacht Prozesse im Speicher und erkennt Malware, die versucht, durch Verschleierungstechniken der Erkennung zu entgehen.
- **Exploit Blocker:** Schützt vor Angriffen, die Sicherheitslücken in häufig genutzten Anwendungen ausnutzen.
- **ESET LiveGrid® Reputation System:** Ein Cloud-basiertes System, das Dateien mit einer ständig aktualisierten Datenbank bekannter Bedrohungen abgleicht.
- **Integriertes Sandboxing:** Die Sandbox hilft dabei, gut getarnte Schadsoftware zu entdecken, indem sie verdächtige Samples in einer isolierten Umgebung ausführt.
- Weitere wichtige Technologien sind UEFI-Scanner und ↗Botnet-Protection.

So machen Sie EDR-Killern das Leben schwer

Leider ist kein EDR völlig immun gegen EDR-Killer. Doch eine Lösung wie die Endpoint Detection & Response von ESET blockiert viele dieser anfälligen Treiber effektiv. ESET Analysten und Administratoren unterstützen Kunden dabei, ihre Abwehr weiter zu verstärken. Der erste wichtige Schritt ist die Konfiguration von PUA (Potentially Unwanted Applications)-Einstellungen. Dadurch werden nur die neuesten Treiber zugelassen.

Eine weitere Möglichkeit, um das Betriebssystem gegenüber Cyberangriffen zu härten, sind Windows Defender Application Control (WDAC)-Regeln. Sie schränken ein, welche Anwendungen Code im Kernel ausführen dürfen und behindern so EDR-Killer. Solche Tricks können einen entscheidenden Unterschied im Umgang mit dieser fiesen Schadsoftware machen.

Zusammenfassung

Ransomware wird auch 2025 eine ernstzunehmende Gefahr für die Cybersicherheit darstellen. Die Bedrohungsakteure passen ihre Taktiken ständig an und entwickeln immer raffiniertere Malware. Das Ende von LockBit und der Aufstieg von RansomHub zeigen, wie sich das RaaS-Ökosystem weiter verändert, in dem Erfolg daran gemessen wird, Partner zu gewinnen und zu halten. Nach der Zerschlagung von LockBit durch die Strafverfolgungsbehörden wechselten viele Kriminelle zu RansomHub, wodurch eine „Machtverschiebung" bei den Hackergruppen stattfand.

Hinzu kommt, dass fortgeschrittene Techniken wie EDR-Killer und die Beteiligung von APT-Gruppen diese Bedrohungen immer komplexer werden lassen. Die Lage ist zwar ernst, aber keineswegs hoffnungslos, wenn Unternehmen sich nicht nur auf reaktive oder wiederherstellende Maßnahmen nach Cyberangriffen konzentrieren. Eine präventive Sicherheitsstrategie wie der „Prevention First"-Ansatz – von ESET kann das Risiko eines erfolgreichen Ransomware-Angriffs deutlich eindämmen. Sie umfasst unter anderem:

- ein robustes Patch- und Schwachstellenmanagement
- eine Zero-Trust-Architektur
- Richtlinien für das Passwortmanagement
- eine Multi-Faktor-Authentifizierung (MFA)
- Mitarbeiterschulungen
- kontinuierliche Bedrohungsüberwachung

IT-Sicherheit ist Vertrauenssache

ESET steht als europäischer IT-Sicherheitsanbieter für höchste Datenschutzstandards, technologische Unabhängigkeit und kompromisslose Transparenz. „Made in EU" ist für uns weit mehr als ein Herkunftssiegel – es ist Ausdruck unserer Verpflichtung gegenüber den Werten der EU, insbesondere im Hinblick auf den Schutz sensibler Daten, die Integrität unserer Technologien und die Sicherstellung digitaler Resilienz.

Als Unternehmen mit Hauptsitz in der Europäischen Union unterliegt ESET vollständig der Datenschutz-Grundverordnung (DSGVO). Unsere Lösungen werden ohne versteckte Zugriffsmöglichkeiten (Backdoors) entwickelt und entsprechen strengen Compliance-Vorgaben.

ESET bietet Informationssicherheit für Unternehmen jeder Größe

Qualitätsmanagement – Made in EU:

- Überall verfügbar – vollautomatischer Schutz der gesamten Organisation
- Volle Kontrolle über Ihre Daten dank transparenter (Sample-)Analysen innerhalb der EU
- Einzigartige Geschwindigkeit bei der Analyse von eingehenden Warnmeldungen
- Zuverlässig und sicher – alle Anforderungen von Datenschutzbestimmungen (bspw. DSGVO) bequem erfüllen
- Große Flexibilität in puncto Vertragsmodell, Hardwareeinsatz und Anforderungen an die Infrastruktur

Vorteile für Unternehmen:

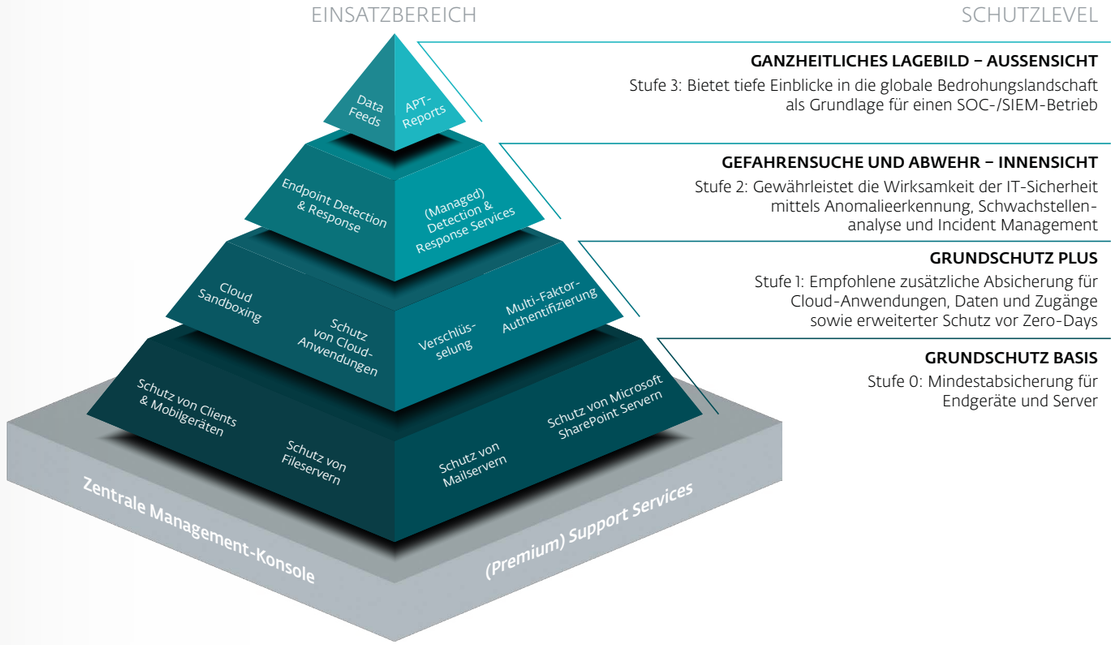
- Passgenaue IT-Sicherheit für alle Unternehmensgrößen und -anforderungen
- Mitarbeiter entlasten und (Hardware-) Ressourcen schonen
- Compliance und Sicherheitsstandards erweitern
- Verwaltung der Schutzlösungen für alle gängigen Betriebssysteme via ESET PROTECT (Cloud oder On-Premises)
- Kombination beliebiger Betriebssysteme (Windows, macOS, Linux) und Geräte (Clients, Server, Mobilgeräte) entsprechend der Bedürfnisse

„Als Security-Hersteller bieten wir moderne Lösungen, Dienstleistungen und Konzepte an, mit denen Unternehmen und Verwaltungen eine Cyber-Resilienz auf höchstem Niveau gestalten können."

— Holger Suhl, Country Manager DACH,
ESET Deutschland GmbH

Zero Trust Security von ESET

Das Zero Trust Security-Konzept von ESET besteht aus einem dreistufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer". Ob als Standardlösung oder als Managed Service - die Kombination aus Endpoint Security, Verschlüsselung, Multi-Faktor-Authentifizierung, Cloud Sandboxing und Schutz für Cloud-Anwendungen bildet dabei das richtige Fundament für Zero Trust.



ESET MDR: Frühzeitig erkennen, schnell reagieren

ESET bietet Managed Detection & Response (MDR) für KMU und Enterprise. Der Service ESET MDR überwacht Ihre Systeme rund um die Uhr. Die Kombination aus KI und menschlicher Kompetenz sorgt für einen erstklassigen Ransomware-Schutz, auch ohne eigene Sicherheitsspezialisten im Haus.

ESET MDR Ultimate bietet Großunternehmen ein effektives Security Operation Center. Die erfahrenen Spezialisten von ESET führen proaktives Threat Hunting und Threat Monitoring durch, unterstützen Sie bei der Analyse von Sicherheitsvorfällen und ergreifen sofort geeignete Maßnahmen.

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

CHAMPION PARTNER

Seit 2019 ein starkes Team auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt

Mehr als 4.000 Postfächer

ISP Security Partner seit 2008

2 Millionen Kunden

BEWÄHRT

Secur IT y made in EU

Trust Seal www.teletrust.de/itsmie

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

Unsere Lösungen sind nach den Qualitäts- und Informations-sicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

178
Länder & Regionen

500.000+
Geschützte Unternehmen

11
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 Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, 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

ESET Digital Security Guide

ESET Deutschland GmbH
Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH