UMFRAGE

Stand der IT-Sicherheit 2023

Digital Security
Progress. Protected.

ESET 100% Made in EU IT-Security

Stand der IT-Sicherheit 2023

ESET führte über einen Zeitraum von drei Monaten eine Umfrage zum Stand der IT-Sicherheit im deutschsprachigen Raum durch. Darin wurde unter anderem eruiert, inwieweit sich der Begriff *Zero Trust Security* unter Resellern und Endkunden etabliert hat und wie die Absicherung der IT-Landschaft in der Praxis tatsächlich umgesetzt wird. Mit den Ergebnissen lässt sich ein Lagebild zum aktuellen Stand der IT-Sicherheit skizzieren. Die Umfrage wird in regelmäßigen Abständen wiederholt, um mögliche Trends aufzeigen, analysieren und beurteilen zu können.

374
Teilnehmer

83,4% - Deutschland
7,8% - Schweiz
8,8% - Österreich

Laufzeit von September bis November 2022

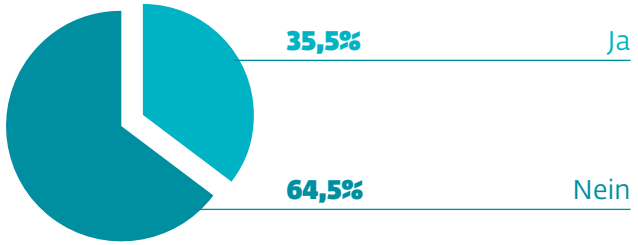
Bedeutsamkeit und aktuelle Herausforderungen von IT-Security in Organisationen

Noch vor einigen Jahren wurde IT-Security in Organisationen eher stiefmütterlich behandelt und insbesondere in vielen kleinen und mittleren Unternehmen oftmals als Projekt bei einem einzelnen Mitarbeiter abgeladen. Mittlerweile entwickelt sich jedoch das Meinungsbild und der Trend, dass IT-Sicherheit Chefsache ist und in die Verantwortung der Führungsetage gehört. Dazu tragen nicht zuletzt rechtliche Regelungen bei, die hohe Anforderungen an Unternehmen stellen und beim Schutz der Systeme die Einhaltung des „Stands der Technik" einfordern. Auch für den Abschluss einer Cyberversicherung rückt das Thema Risikominimierung in den Fokus der Unternehmens-IT. Bei der Umsetzung stehen Organisationen allerdings vor verschiedenen Herausforderungen.

Das tägliche Leben wird immer schneller, immer digitaler. Durch neue Technologien und die zunehmende Vernetzung wird unser Leben einerseits einfacher, anderseits aber auch herausfordernder. Das gilt insbesondere für die moderne Arbeitswelt – schließlich ist ein Geschäftsleben ohne IT kaum noch vorstellbar. Man denke allein an die Unmengen an Daten, die täglich generiert, verarbeitet und geteilt werden. Sowohl der Schutz solcher Daten als auch der Umgang damit haben einen großen Einfluss auf den digitalen Arbeitsalltag. Gleiches gilt ganz grundlegend für die Sicherheit der genutzten Technologien. Denn werden Systeme oder Prozesse kompromittiert oder lahmgelegt, kann das den Geschäftsbetrieb einschränken oder gar zu einem Totalausfall führen, was weitreichende Konsequenzen für die Organisation mit sich bringt.

Betreuung durch Dienstleister

Etwas mehr als ein Drittel (35,5%) der befragten Endkunden gibt ihre IT-Sicherheit in die Hände eines Dienstleisters, während die Mehrheit (64,5%) sich selbst darum kümmert.



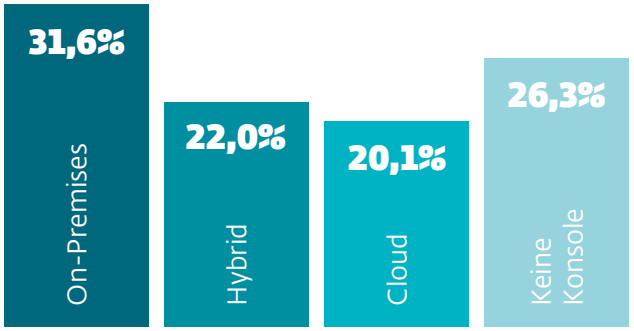
75%

sind aktuell überzeugt, dass IT-Security den richtigen Stellenwert in ihrer Organisation einnimmt

Mit einer Umfrage zum Stand der IT-Sicherheit ist ESET der Frage auf den Grund gegangen, wie es in der Praxis um die Absicherung der IT-Landschaft in Organisationen im deutschsprachigen Raum bestellt ist und welche Herausforderungen Verantwortlichen in diesem Zusammenhang begegnen. Die Ergebnisse decken sich mit der medialen Wahrnehmung der zunehmenden Relevanz von IT-Sicherheit. Knapp Dreiviertel der Umfrageteilnehmer (74,6%) sind überzeugt, dass sie sich bei diesem Thema auf dem richtigen Weg befinden und der Schutz der Systeme innerhalb ihrer Organisation den richtigen Stellenwert einnimmt.

Zentrale Management-Konsole

Knapp ein Drittel der Organisationen (31,6%) setzt auf eine reine Vor-Ort-Management-Konsole (On-Premises), um ihre Sicherheitslösungen zu verwalten. Während 22% einen Mischbetrieb von Cloud und On-Premises im Einsatz haben, setzen 20,1% auf eine reine Cloud-Verwaltung. Ganze 26,3% verwalten ihre Lösungen ohne ein zentrales Management.



47%

beklagen einen Mangel an Personal und/oder finanziellen Ressourcen

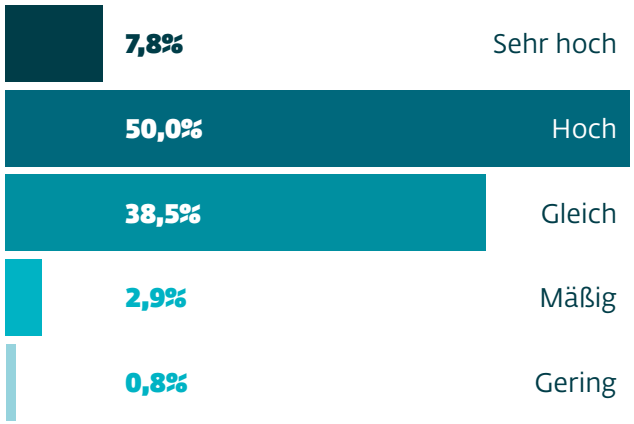
Das Bewusstsein für die Relevanz von IT-Sicherheit ist jedoch nur der erste Schritt. Mit der Planung und Umsetzung ergeben sich viele Herausforderungen, die auch von den Umfrageteilnehmern wahrgenommen werden. Fehlende Budgets und Fachkräftemangel sind hier zwei Schlagwörter, welche die meisten vermutlich nicht zum ersten (und auch nicht zum letzten) Mal hören und auch in der IT-Security-Branche allgegenwärtig sind. So zeigt sich, dass nahezu die Hälfte der Befragten (46,8%) Probleme bei der Umsetzung ihrer IT-Projekte hat, da es schlichtweg nicht genügend finanzielle oder personelle Ressourcen im Unternehmen gibt. Hinzu kommt, dass durch die ständige Weiterentwicklung von Technologien und (einzuhaltenden) Richtlinien ein permanenter Wissenserwerb notwendig ist. So gibt ein Drittel der Befragten (31,6%) an, dass zwar genügend finanzielle und personelle Ressourcen vorhanden sind, es aber an Qualifikations- bzw. Fortbildungsmöglichkeiten mangelt. Vor diesem Hintergrund ist nicht verwunderlich, dass sich nur 14,4% mit ihren derzeit eingesetzten Sicherheitslösungen uneingeschränkt den aktuellen Bedrohungen gegenüber gewachsen sehen.

14%

sehen sich aktuellen Bedrohungen gegenüber vollumfänglich gewappnet

Finanzieller Bedarf in den kommenden drei Jahre

Beim Blick in die Zukunft gaben 57,8% der Organisationen an, dass sie den zusätzlichen finanziellen Bedarf für IT-Security in den nächsten drei Jahren für „hoch“ bzw. „sehr hoch“ einschätzen. Für 38,5% gibt es keinen Grund die finanziellen Mittel zu erhöhen.



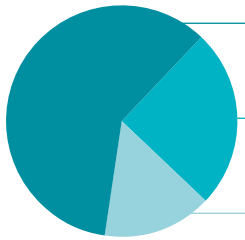
91%

empfinden Zero Trust Security als Orientierungshilfe zur Umsetzung nützlich

Was können Verantwortliche also tun, um das Sicherheitsniveau in ihrer Organisation zu verbessern? Ein erster Schritt besteht darin, den eigenen Schutzbedarf zu identifizieren. Im Dschungel der IT-Sicherheitslösungen kann es unter Umständen schwierig sein, sich zu orientieren und einen klaren Überblick zu bekommen. Hier bietet der mehrstufige Zero Trust Security-Ansatz von ESET die passende Unterstützung. Aufbauend auf der zumeist vorhandenen Mindestabsicherung von Endgeräten und Servern folgen weitere Stufen, die sich am individuellen Schutzbedarf einer Organisation orientieren und das Sicherheitsniveau schrittweise steigern. 90,6% der Umfrageteilnehmer gaben an, dass dieses Modell als Orientierungshilfe absolut geeignet sei. Dabei hilft ein solches Stufenmodell nicht nur bei der Identifizierung von geeigneten bzw. notwendigen Sicherheitslösungen, sondern trägt auch dazu bei, dass die hierfür erforderlichen Budgets besser überblickt und bei der Planung einkalkuliert werden können. Darüber hinaus beleuchtet das Modell mit dem Thema Services eine Möglichkeit, dem anhaltenden Fachkräftemangel zu begegnen. So können Teile oder die gesamte IT-Security an externe Sicherheitsexperten ausgelagert werden (z.B. MDR- oder operative Services), um die eigenen Ressourcen zu schonen.

Bevorzugte Lizenzierungsart

Klassische Laufzeitlizenzen (beispielsweise drei Jahre) ohne automatische Verlängerung ist die attraktivste Lizenzierungsart.



59,8% Laufzeitlizenzen

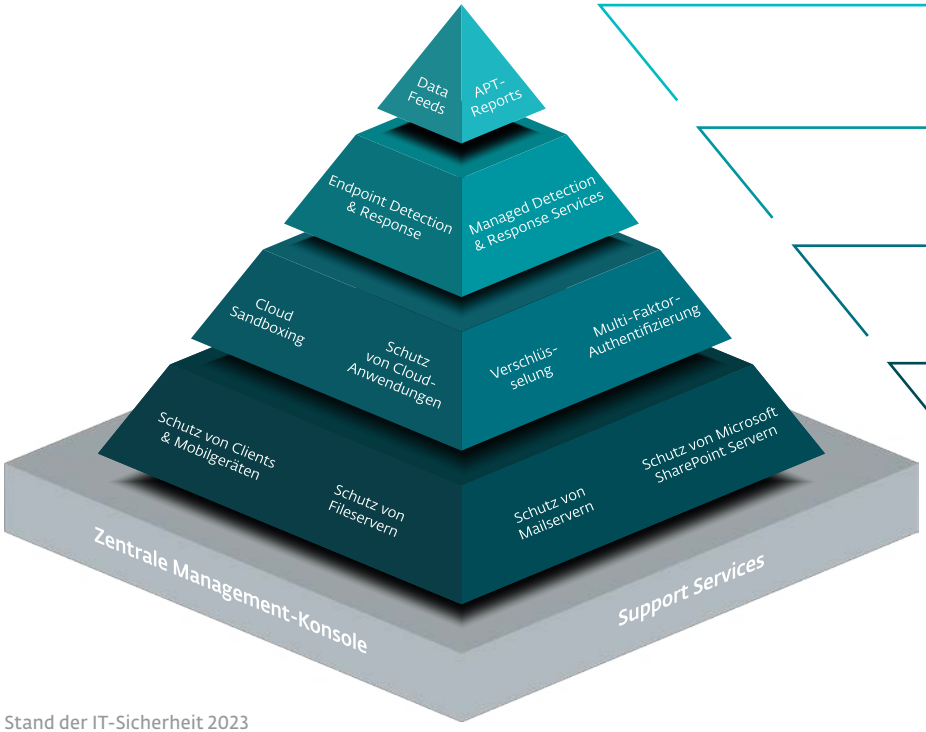
25,0% Monatlich via MSP

15,2% Subscription

Zero Trust Security – die einzelnen Schutzlevel

Bei der Frage, in welcher Stufe sich die jeweilige Organisation aktuell befindet, sahen sich 24,3% in Stufe 0 „Grundschutz Basis“, welche lediglich die Mindestabsicherung der Endgeräte und Server vorsieht. Der Großteil (44,1%) sieht sich in Stufe 1 „Grundschutz Plus“, das zusätzlichen Schutz von Cloud-Anwendungen, Daten und Zugängen sowie erweiterten Schutz vor Zero Days bietet. Etwas mehr als ein Viertel (26,5%) ordnet sich in Stufe 2 „Gefahrensuche und Abwehr – Innensicht“ ein, das sich durch Anomalieerkennung, Schwachstellenanalyse und Incident Management auszeichnet.

EINSATZBEREICH



SCHUTZLEVEL

5,1%

GANZHEITLICHES LAGEBILD – AUSSENSICHT

Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb

26,5%

GEFAHRENSUCHE UND ABWEHR – INNENSICHT

Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, Schwachstellenanalyse und Incident Management

44,1%

GRUNDSCHUTZ PLUS

Stufe 1: Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero Days

24,3%

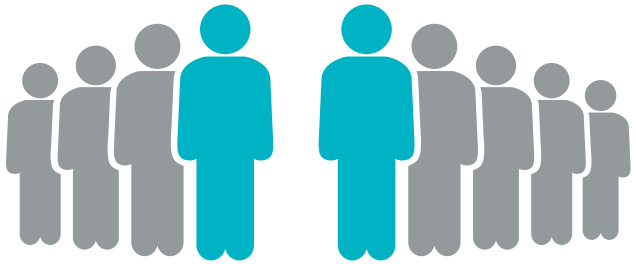
GRUNDSCHUTZ BASIS

Stufe 0: Mindestabsicherung für Endgeräte und Server

Deutlich weniger Organisationen (5,1%) sehen sich in der höchsten Ausbaustufe „Ganzheitliches Lagebild – Außensicht". Hier werden APT-Reports und Data Feeds herangezogen, um tiefe Einblicke in die globale Bedrohungslandschaft zu erhalten. Bei der Bewertung dieser Antworten muss natürlich berücksichtigt werden, dass die IT-Umgebung einer Organisation einen maßgeblichen Einfluss darauf hat, welche Sicherheitslösungen notwendig und sinnvoll sind. Ein Unternehmen, das keinen Mail Server einsetzt, benötigt auch keine entsprechende Sicherheitssoftware. Gleiches gilt für den Einsatz von Cloud-Anwendungen wie Microsoft 365 und etwaigen Schutzlösungen. Zudem sollten verschiedene weitere Faktoren wie Unternehmensgröße, Branchenzugehörigkeit und Gefahrenpotenzial bei der Frage nach der Angemessenheit von Sicherheitslösungen und -strategien berücksichtig werden. So gehören zum Beispiel Threat Intelligence Services sicherlich nicht zu den Standardmaßnahmen, die man von allen Organisationen pauschal einfordern würde.

Einsatz von Endpoint Detection and Response Lösungen

Jede vierte Organisation setzt bereits eine EDR-Lösung ein, jede fünfte sogar in Verbindung mit MDR-Services.



1 von 4
EDR-Lösungen

1 von 5
MDR-Services

Digital Security
Progress. Protected.

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.

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

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

Trust Seal
www.teletrust.de/itsmie

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

Unsere Lösungen sind nach den Qualitäts- und
Informationssicherheitsstandards ISO 9001:2015
und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

195
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

Digital Security
Progress. Protected.

ESET.DE | ESET.AT | ESET.CH

Stand: 05/2023