IN 6 SCHRITTEN ZU MEHR IT-SICHERHEIT. **EIN GUIDE FÜR START-UPS.**

IT ist überall. Auch kleine Unternehmen und Start-ups kommen heute längst nicht mehr ohne PCs, Smartphones, Server und Co. aus. Einige der damit verbundenen Risiken, wie der Diebstahl physischer Gegenstände oder Geräteausfälle durch Naturkatastrophen, lassen sich durch durchdachte Vorsichtsmaßnahmen und entsprechendes Verhalten zwar nicht verhindern, aber doch wesentlich verringern. Ungleich komplizierter ist der Umgang mit Risiken, die durch Cyberkriminalität entstehen. Dazu zählen beispielsweise der gezielte Diebstahl von Informationen oder Daten und deren Verkauf im Darknet. Datenschutzvorfälle in Deutschland passieren gerade nicht nur in Großkonzernen, sondern eben auch in kleinen und mittelständischen Unternehmen.

Nichtsdestotrotz glauben viele Verantwortliche bis heute, dass ihre Firma aufgrund der geringen Größe und der vermeintlich wenig wertvollen Daten für Angreifer nicht interessant wäre. Ein Trugschluss mit teils dramatischen Folgen. Die folgenden Hinweise sollen Ihnen helfen, Ihr Unternehmen wirksam und nachhaltig vor den Folgen von Cyberkriminalität zu schützen. Personenbezogene Daten, also solche, die beispielsweise für Identitätsdiebstahl und -betrug verwendet werden können, sind für Kriminelle besonders attraktiv. Selbst kleinste Unternehmen verarbeiten diese Art Informationen, z.B. in Kunden- oder Lieferantendatenbanken. Ebenfalls lohnenswerte Ziele sind Zahlungsinformationen, Kreditkartendaten, Kontodaten, Passwörter für Onlinebanking und E-Mail-Accounts sowie Zugangsdaten zu Online-Diensten wie eBay oder PayPal. Die erbeuteten Daten werden dann meist im Darknet an Dritte verkauft, die sie wiederum für ihre kriminellen Machenschaften missbrauchen.

Datenlecks und ihre Folgen

Eines sollten Sie immer im Hinterkopf behalten: Als Unternehmen sind Sie allein für die Sicherheit der durch Sie verarbeiteten Daten verantwortlich. Egal, ob Zugangsinformationen, Kontakt- oder andere sensible Daten: Werden diese aus Ihren Systemen gestohlen und zum Beispiel für Identitätsbetrug missbraucht, können letztlich Sie dafür haftbar gemacht werden. Dies gilt insbesondere für personenbezogene Daten, die durch spezielle Gesetze und Verordnungen geschützt sind, zum Beispiel die DSGVO in Deutschland oder der CCPA in den USA (Kalifornien). Egal, ob verloren gegangener Laptop mit Kundendaten oder USB-Stick mit Patienteninformationen: Viele Datenschutzgesetze fordern nicht nur, dass Unternehmen den Schutz von sensiblen Daten sicherstellen. Treten Datenschutzvorfälle und Datenlecks auf, müssen diese zudem umgehend an die entsprechenden Behörden gemeldet werden. In der Praxis heißt das, dass selbst kleine Unternehmen die Ihnen anvertrauten Daten systematisch absichern müssen. Dazu gehört unter anderem auch die Dokumentation der getroffenen Maßnahmen – nicht nur für potenzielle Meldungen an Behörden. Auch die Schulung von Mitarbeitern in Sachen Datenschutz wird wesentlich leichter, wenn Sie im Voraus nachvollziehbar dokumentiert haben, was in Sachen Datenschutz zu tun ist. Größere Unternehmen fordern zudem von ihren kleineren Zulieferern oftmals Nachweise darüber, dass diese ihre Mitarbeiter umfassend zum Thema Datenschutz geschult haben und dass Maßnahmen zum Schutz von Daten im Unternehmen umgesetzt werden. Nicht zuletzt helfen Ihnen schriftlich niedergelegte Datenschutzrichtlinien, im Fall der Fälle gegenüber den Datenschutzbehörden nachzuweisen, dass Sie alle Erfordernisse für den Schutz personenbezogener Daten erbracht haben.

In 6 Schritten zu mehr Cybersicherheit

Sie sehen also: Ohne systematische Cybersecurity geht es längst nicht mehr. Folgen Sie unseren Schritten 1 bis 6, um den Schutz Ihrer sensiblen Daten und die IT-Sicherheit Ihres Unternehmens Schritt für Schritt zu erhöhen.

ASSESS – Dokumentieren Sie Ihre Assets, Risiken und Ressourcen

BUILD – Stellen Sie Sicherheitsrichtlinien auf

CHOOSE – Wählen Sie passende Kontrollmechanismen

DEPLOY – Implementieren Sie die Kontrollmechanismen

EDUCATE – Schulen Sie Mitarbeiter, Führungskräfte und Zulieferer

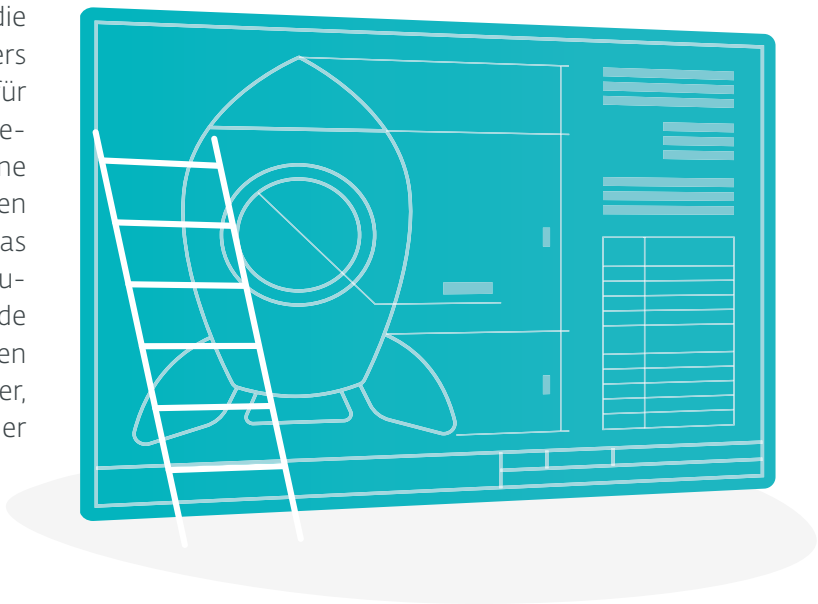
FURTHER – Weiterführende Dokumentation, Prüfung, Tests

1. ASSESS – Dokumentieren Sie Ihre Assets, Risiken und Ressourcen

Die Grundannahme ist einfach: Nur die Dinge, von denen Sie wissen, dass Sie da sind, können Sie auch schützen. Dokumentieren Sie also Ihre komplette IT-Infrastruktur. Listen Sie alle Geräte und Services auf, die im Unternehmen genutzt werden. Besonderes Augenmerk sollten Sie dabei auch auf Mobilgeräte wie Smartphones und Tablets legen, mit denen Ihre Mitarbeiter oder Sie selbst auf personenbezogene Daten Ihrer Kunden zugreifen (können). Gerade für Mobilgeräte haben viele Unternehmen nämlich noch immer keine gültigen Richtlinien für den sicheren Umgang formuliert. Bestehen diese, werden sie aber aus Zeit- und vermeintlichen Effizienzgründen nicht selten umgangen. Listen Sie unbedingt auch Online-Dienste auf, die Sie im Unternehmen nutzen, z.B. SalesForce, Cloud-Dienste wie iCloud oder Google Docs sowie Bankwebseiten für Onlinebanking. Im nächsten Schritt begutachten Sie die einzelnen Punkte auf der Liste und prüfen, welche Risiken damit jeweils verbunden sind. Wer oder was könnte eine potenzielle Gefahr im Zusammenhang mit dem Gerät oder Dienst werden? Welche Risiken ergeben sich, wenn das Gerät außerhalb des Unternehmensnetzwerks verwendet oder der Service remote aufgerufen wird? Immer eine gute Frage ist außerdem: "Was könnte schiefgehen?" Manche Risiken sind dabei sicherlich wahrscheinlicher als andere. Dennoch sollten Sie alle auflisten und sortieren: Wie wahrscheinlich ist es, dass das Risiko eintritt? Welcher Schaden würde entstehen, wenn dies passiert? Die Dokumentation Ihrer IT-Assets bildet die Grundlage aller weiteren Punkte und sollte besonders sorgfältig durchgeführt werden. Haben Sie hierfür nicht ausreichend Kapazitäten, suchen Sie sich gegebenenfalls Hilfe. Hierfür benötigen Sie zunächst eine weitere Liste, auf der Sie alle verfügbaren Ressourcen im Unternehmen für solche Aufgaben aufführen. Das können zum einen Mitarbeiter sein, die in IT- und Security-Fragen bewandert sind oder aber entsprechende Geschäftspartner oder Zulieferer. Bei Bedarf lassen sich Cybersecurity-Aufgaben an externe Dienstleister, zum Beispiel sogenannte Managed Service Provider (MSP) auslagern.

2. BUILD – Stellen Sie Sicherheitsrichtlinien auf

Die Basis starker Cybersecurity sind und bleiben durchdachte Sicherheitsrichtlinien. Diese können aber nur dann bei den Mitarbeitern ankommen, wenn sie auch auf oberster Ebene umgesetzt werden. Fassen Sie sich zunächst an die eigene Nase: Wo können Sie Ihr Verhalten ändern, um die Sicherheit der Ihnen anvertrauten Daten zu erhöhen? Zeigen Sie Ihren Mitarbeitern, wie ernst es Ihnen um die IT-Sicherheit des Unternehmens und den Schutz der Daten Ihrer Kunden, Geschäftspartner und Mitarbeiter ist. Nun ist es an der Zeit, die Vorgaben zum Schutz sensibler Daten in Regeln auszuformulieren. Verbieten Sie zum Beispiel den Zugriff nicht autorisierter Dritter auf Unternehmenssysteme und -daten und legen Sie fest, dass Mitarbeiter die Sicherheitseinstellungen der genutzten Mobilgeräte nicht verändern können. Ebenso Bestandteil der Richtlinien sollte die Vergabe von Rechten sein, die einzelne Mitarbeiter/Rollen oder Gruppen bekommen. Wer bekommt Zugriff auf welche Daten, für welchen Zweck und was genau können sie mit den Daten tun? Weitere Punkte, für die Sie Security-Vorgaben entwickeln sollten: Remote-Zugriff auf Unternehmenssysteme, private Geräte der Mitarbeiter, welche sie für Arbeitszwecke verwenden sowie zugelassene Software.



3. CHOOSE – Wählen Sie passende Kontrollmechanismen

Die besten Vorgaben nutzen wenig, wenn Mechanismen fehlen, die ihre Umsetzung überwachen. Um den Zugriff unbefugter Dritter auf Unternehmensnetzwerke und -daten bestmöglich zu verhindern, sollten Verschlüsselung der Daten als auch eine Zugangskontrolle in Form einer Multi-Faktor-Authentifizierung zum Einsatz kommen. Um zu verhindern, dass nicht zugelassene Programme auf Unternehmensrechnern ausgeführt werden, vergeben Sie keine Administratorrechte an Mitarbeiter, die diese nicht für ihre Arbeitsaufgaben benötigen. Um sicherzustellen, dass verloren gegangene oder gestohlene Geräte keine Datenlecks verursachen, verpflichten Sie Mitarbeiter, derartige Vorfälle umgehend zu melden. Legen Sie fest, dass Ihre IT-Abteilung das betroffene Gerät sofort sperrt und darauf enthaltene Daten per Fernzugriff entfernt. Eine gute Auswahl an Security-Lösungen erleichtert Ihnen das Leben zusätzlich. Mindestens sollten Sie jedoch grundlegende Technologien implementieren:

- Eine zuverlässige Endpoint Security, welche die einzelnen Geräte (Endpoints) im Unternehmen vor Malware schützt,
- eine Verschlüsselungslösung, durch die selbst Daten auf gestohlenen Geräten für Kriminelle unbrauchbar werden
- eine Multi-Faktor-Authentifizierung, sodass Zugänge und Daten nicht bloß per Nutzername und Passwort gesichert sind,
- sowie eine VPN-Lösung, die auch das Arbeiten von Zuhause und anderswo absichert.

Sichere Daten – heute und in Zukunft

Die Zahl und Arten an Bedrohungen nehmen ständig zu. Cyberkriminelle entwickeln immer neue Methoden, Nutzer und Sicherheitssysteme zu täuschen und so unbemerkt in Netzwerke zu gelangen. Mit einer cloudbasierten Sandbox, die selbst bisher unbekannte Bedrohungen zuverlässig erkennt, sichern Sie Ihre Unternehmens-IT auch gegenüber zukünftigen Angriffen umfassend ab. So wird beispielsweise selbst bisher noch nie dagewesene Ransomware erkannt und daran gehindert, auf dem Endpoint ausgeführt zu werden.

Weitere Infos und Tipps zum Thema Endpoint-Security:

Der Schutz Ihrer Endgeräte ist einer der wichtigsten Bestandteile eines mehrschichtigen IT-Sicherheitskonzepts in Ihrem Unternehmen. Deshalb sollten Sie eine Endpoint-Security-Lösung auswählen, die zu Ihrem Unternehmen passt, zuverlässig ist, Ihre Systeme nicht beeinträchtigt und es Ihnen ermöglicht, sich auf das zu konzentrieren, was wichtig ist: Ihr Business! Um die verschiedenen Angebote auf dem Markt zu bewerten kann es hilfreich sein, Bewertungen und Erfahrungsberichte zu lesen. Dabei ist es wichtig auf bestimmte Punkte zu achten.

- **Erkennungsraten:** Die wichtigste Fähigkeit von Cybersecurity-Software ist das Erkennen von Bedrohungen. Die Erkennungsraten sollten so hoch wie möglich sein.
- **Fehlalarme:** Ein Fehlalarm kann ernsthafte Probleme verursachen. Beispielsweise dann, wenn eine Antivirenlösung so konfiguriert ist, dass infizierte Dateien sofort gelöscht oder unter Quarantäne gestellt werden. Eine fälschlicherweise als Malware identifizierte wichtige Datei kann dann etwa dazu führen, dass Anwendungen oder gar ganze Betriebssysteme funktionsunfähig werden. Und selbst, wenn Fehlalarme Ihr System nicht zum Stillstand bringen, werden IT-Ressourcen unnötig gebunden um die Dateien zu Überprüfen und ggf. Systeme wiederherzustellen. Wiederholte Fehlalarme führen auch dazu, dass Alarme generell weniger ernst genommen werden. Fehlalarme erhöhen somit indirekt die Wahrscheinlichkeit, dass Malware ernsthaften Schaden anrichtet.
- **Systemanforderungen:** Cybersecurtiy-Software bindet einen Teil der Ressourcen des Computers. In Anbetracht der Work-From-Home (WFH) Situation, sowie der Nutzung von Laptops und Notebooks, sollten die begrenzten Ressourcen des Rechners so wenig wie möglich beeinträchtigt werden.
- **Verwaltung und Wartung:** Das Management der Vielzahl an Endgeräten die in Unternehmens eingesetzt werden, sollte der Einfachheit halber über eine zentrale Konsole möglich sein. Durch eine cloudbasierte Konsole kann dies sogar von jedem beliebigen Netzwerk aus geschehen.
- **Support**: Alle wichtigen Informationen sollten immer verfügbar sein. Im Idealfall sortiert innerhalb einer Wissensdatenbank. Falls wegen eines Sicherheitsvorfalls dringend ein Spezialist benötigt wird ist ein schnell erreichbarer Support unabdingbar.

4. DEPLOY – Implementieren Sie die Kontrollmechanismen

Sorgen Sie dafür, dass die Mechanismen wirklich funktionieren und Ihre Sicherheitsrichtlinien einhalten. Es reicht aber nicht aus, lediglich die Lösungen zu installieren und zu überprüfen, ob sie die Geschäftsprozesse nicht stören. Vielmehr müssen Sie sicherstellen, dass diese in der Praxis das erforderliche Schutzniveau bieten. Regelmäßige Penetrationstests haben sich dafür bestens bewährt. Ein Penetrationstest ist ein beauftragter, geplanter und simulierter Cyberangriff auf ein Unternehmen. Damit möchte man bisher unbekannte Angriffspunkte oder Sicherheitslücken identifizieren und eliminieren. So können Sie verhindern, dass Hacker später sensible Daten stehlen oder Ihr Start-up anderweitig schädigen.

Verwaltungskonsole für Endpoint Security

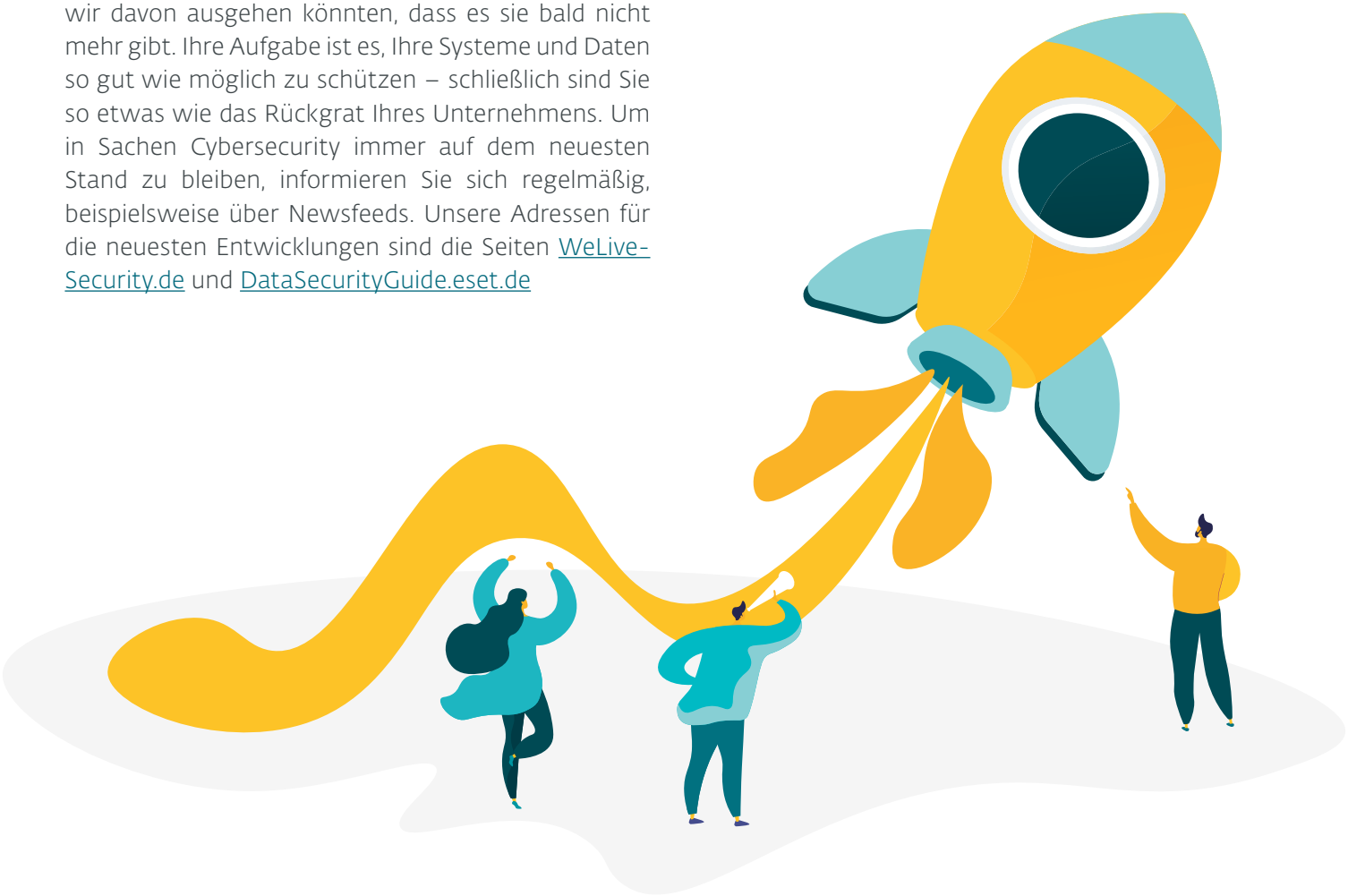
ESET PROTECT bietet den vollen Überblick in einer einzigen Konsole. Damit erhalten Sie oder Ihre Admins nicht nur Einblick in die Security aller Endpoints im Unternehmen und an mobilen Arbeitsplätzen, sondern liefert dazu bei Bedarf umfangreiche Reportings und Verwaltungsfunktionen – unabhängig vom jeweils installierten Betriebssystem. So haben Sie jederzeit Einblick in alle Vorbeuge-, Erkennungs- und Abwehrmaßnahmen auf DesktopPCs, Servern, VMs und sogar Mobilgeräten.

5. EDUCATE – Schulen Sie Mitarbeiter, Führungskräfte und Zulieferer

Nun sind die Sicherheitsrichtlinien aufgestellt und für jeden Mitarbeiter jederzeit einsehbar. Sie haben sie sogar verpflichtet, sich diese genau anzuschauen und zu verinnerlichen. Sie ahnen es: Für eine wirklich umfassende IT-Sicherheitsstrategie reicht das nicht. Ihre Mitarbeiter müssen verstehen, warum welche Vorgaben und Richtlinien nötig sind. Investieren Sie in die Schulung Ihrer Mitarbeiter. Ziel ist es, die sogenannte Security Awareness aller Mitarbeiter zu erhöhen, also ihre Sensibilität für Themen rund um die Sicherheit der IT-Systeme zu verbessern. Dies ist letzten Endes die wichtigste Maßnahme, die Sie treffen können, um die IT-Sicherheit Ihres Unternehmens zu verbessern. Klären Sie Ihre Mitarbeiter umfassend auf. Implementieren Sie regelmäßige Trainings für Ihre Mitarbeiter, beispielsweise kleine Quizze zum Thema Phishing-Angriffe, um sie über typische Merkmale von manipulierten E-Mails aufzuklären. Integrieren Sie Security Awareness-Maßnahmen ins Onboarding neuer Mitarbeiter und veröffentlichten Sie regelmäßige Security-Tipps auf der Startseite Ihres Intranets. Stellen Sie sicher, dass Ihre Schulungsmaßnahmen wirklich jeden erreichen, der in Ihrem Netzwerk unterwegs ist – seien es Mitarbeiter, Führungskräfte, Zulieferer oder Partner. Nutzen Sie mögliche Zuwiderhandlungen, um Ihre Security Richtlinien regelmäßig zu überprüfen und eventuellen Nachschulungsbedarf zu erkennen.

6. FURTHER – Weiterführende Dokumentation, Prüfung, Tests

Der Aufbau einer zuverlässigen IT-Security ist tatsächlich niemals abgeschlossen. Planen Sie deshalb regelmäßige – mindestens einmal jährliche – Audits für Ihre Maßnahmen ein. Möglicherweise stellt sich dabei heraus, dass einzelne Vorgaben oder Kontrollmechanismen überarbeitet werden müssen, weil sich die äußeren Umstände oder interne Gegebenheiten geändert haben, seien es Veränderungen in der Branche, neue Geschäftsbeziehungen, neue Projekte, neue Mitarbeiter oder der Verlust früherer Mitarbeiter. (Sorgen Sie beim Weggang von Mitarbeitern unbedingt dafür, alle Zugänge zu internen Systemen umgehend zu sperren.) Eventuell kann es sich als nützlich erweisen, externe Experten mit Penetrationstests oder dezidierten Security Audits zu beauftragen, um Schwachstellen in Ihrer IT-Sicherheitsstrategie gezielt ausfindig zu machen und angehen zu können. Eines steht fest: Cyberkriminalität ist zu lukrativ, als dass wir davon ausgehen könnten, dass es sie bald nicht mehr gibt. Ihre Aufgabe ist es, Ihre Systeme und Daten so gut wie möglich zu schützen – schließlich sind Sie so etwas wie das Rückgrat Ihres Unternehmens. Um in Sachen Cybersecurity immer auf dem neuesten Stand zu bleiben, informieren Sie sich regelmäßig, beispielsweise über Newsfeeds. Unsere Adressen für die neuesten Entwicklungen sind die Seiten WeLive-Security.de und DataSecurityGuide.eset.de



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 Entwicklungs-zentren weltweit

welivesecurity by eset