Angriff ist nicht gleich Untergang: **Die hohe Kunst der Cyber-Resilienz**

Digitale Prophylaxe stärkt eigene Security und bewahrt die Geschäftskontinuität

Cyberangriffe gehören heute zu den größten Bedrohungen für Organisationen jeglicher Größe. Die Folgen können verheerend sein, von finanziellen Verlusten bis hin zu Rufschäden und langfristigen Auswirkungen auf das Geschäft. Mit proaktiven Maßnahmen stärken Firmen und Verwaltungen ihre digitale Widerstandskraft und bereiten sich auf den Ernstfall vor.

Unternehmen und Institutionen sind immer wieder mit Sicherheitsvorfällen konfrontiert. Laut dem Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Bedrohungslage so hoch wie nie zuvor. Ransomware gilt als die größte Bedrohung, wobei eine Verlagerung der Attacken beobachtet wurde. Nicht nur große Unternehmen, sondern auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen wurden zunehmend Ziel von Cyberangriffen. Beispielsweise wurde Ende 2023 der IT-Dienstleister Südwestfalen IT von einem Ransomware-Angriff betroffen, der mindestens 103 Kommunen in Nordrein-Westfalen zum Teil wochenlang offline gehen ließ.

CYBER-RESILIENZ BEWAHRT VOR DEM DIGITALEN SUPER-GAU

Ohne Wenn und Aber müssen Organisationen die eigene Widerstandskraft gegen digitale Angriffe stärken. Experten sprechen in diesem Zusammenhang von der Cyber-Resilienz (CR). Darunter versteht man die Fähigkeit einer Organisation, trotz Hackerangriffen oder anderen IT-Störungen ihre Tätigkeiten aufrechtzuerhalten und Geschäftsziele zu erreichen. Cyber-Resilienz ist nicht nur eine technische Herausforderung, sondern erfordert auch eine organisatorische Vorbereitung auf mögliche IT-Notfälle. Dazu bedarf es einer gut geplanten Strategie, um im Ernstfall schnell und effektiv reagieren zu können und Schäden zu minimieren - und die Fähigkeit, Prozesse angesichts neuer Gefahren kontinuierlich anzupassen. Ein Schlüsselelement ist dabei die Auseinandersetzung mit und ein tiefgehendes Verständnis von Risiken. Sie bestimmen, welchen technischen Maßnahmen und Prozesse zum Ziel führen.

DER UNTERSCHIED VON CYBER-RESILIENZ UND CYBER-SECURITY

Cyber-Resilienz und Cyber-Security sind verwandte Begriffe. Allerdings ist die der Cyber-Resilienz wesentlich weiter gefasst. Hierbei handelt es sich um einen ganzheitlichen Ansatz, der neben der Cyber-Security weitere Aspekte berücksichtigt wie das Business Continuity Management, Incident Response und Disaster Recovery. Während die Cyber-Security eher technische Verfahren und Prozesse definiert (wie beispielsweise Firewalls, VPN, Anti-Malware etc.), die IT-Infrastruktur mit ihren Systemen, Netzen und Daten vor digitalen Angriffen zu schützen, geht die Cyber-Resilienz einen Schritt weiter und sieht Verfahren, Schritte und Prozesse vor, die Geschäftsabläufe während eines Angriffs aufrechtzuerhalten oder nach einem Vorfall möglichst schnell wieder aufzunehmen.

Um die digitale Widerstandskraft zu erhöhen, können Organisationen verschiedene Vorkehrungen ergreifen, wie zum Beispiel:

- Ein Cyber-Resilienz-Managementsystem implementieren, das auf internationalen Standards wie ISO/IEC 27001 oder BSI TR-03183 basiert und die Sicherheit, Verfügbarkeit und Wiederherstellbarkeit der IT-Systeme und -Daten gewährleistet.
- Regelmäßig Cyber-Resilienz-Übungen durchführen, um die Wirksamkeit der Strategie und des Managementsystems zu testen, die Mitarbeiter zu schulen und zu sensibilisieren, und die Lücken und Verbesserungsmöglichkeiten zu identifizieren.
- Kontinuierlich die Cyber-Resilienz überwachen, bewerten und verbessern, indem man die aktuellen Trends und Entwicklungen im Bereich der Cyber-Sicherheit verfolgt, Kennzahlen analysiert und die notwendigen Anpassungen vornimmt.
- Eine IT-Notfallkarte erstellen, die die wichtigsten Informationen und Anweisungen für den Fall eines IT-Notfalls enthält, wie zum Beispiel die Kontaktdaten der IT-Notfallverantwortlichen, die Eskalationswege, die Erstmaßnahmen und die Wiederanlaufpläne.

Doch der Weg dorthin ist nicht so einfach, wie diese vier vorgestellten Beispiele möglicherweise suggerieren. Eine Gesamtstrategie beinhaltet eine Vielzahl von Aktivitäten in personeller, sicherheits- und prozesstechnischer Hinsicht.

Personelle Maßnahmen

SICHERHEITSBEWUSSTSEIN SCHAFFEN

Mitarbeiter sind oft das schwächste Glied in der Sicherheitskette. Schulungen und Sensibilisierungskampagnen sind daher entscheidend, um das Sicherheitsbewusstsein der Mitarbeiter zu stärken und sie für die Risiken von Cyberangriffen zu sensibilisieren. Unternehmen sollten ihre Mitarbeiter regelmäßig über aktuelle Bedrohungen informieren sowie an praxisnahen Beispielen Gefahren erkennen und Abwehrmaßnahmen einleiten.

EXPERTEN MIT INS BOOT HOLEN

Auch die schonungslose Analyse der eigenen IT-Security-Abteilung steht auf dem Plan. Es ist höchst wahrscheinlich, dass aufgrund von schmalen Budgets und dem Fachkräftemangel das Team nicht ausreichend stark besetzt oder das Know-how entwicklungsfähig ist. Nicht jeder IT-Administrator ist auch gleich ein Security-Experte. Mit Managed Security Service Providern oder Managed Detection and Response-Dienstleistungen von IT-Sicherheitsherstellern stehen bezahlbare externe Fachleute zur Verfügung.

Prozesse neu überdenken

RISIKOBEWERTUNG UND -MANAGEMENT: IDENTIFIZIERUNG VON ANGRIFFSFLÄCHEN

Als zentraler Baustein der Cyber-Resilienz gilt der Umgang mit Risiken. Die Risikobewertung und -managementprozesse sind entscheidend für die Stärkung der eigenen Widerstandskraft. Diese Prozesse umfassen die systematische Identifizierung, Bewertung und Priorisierung von potenziellen Gefahren sowie die Entwicklung und Implementierung von Strategien zur Risikominderung. Um dies alles überhaupt vornehmen zu können, muss man die eigentlichen Angriffsflächen bzw. Gefahrenherde kennen.

Identifikation von Angriffsflächen

Viele Organisationen konzentrieren sich vornehmlich auf den Schutz des eigenen Netzwerks mit gängigen Mitteln von Malwareschutz bis Cloud Sandboxing. Im Vorfeld werden aber zu selten die individuellen Angriffsflächen untersucht: also potenziellen Schwachstellen in den eigenen Systemen und Prozessen, die von Angreifern ausgenutzt werden könnten. Angriffsflächen können vielfältig sein und umfassen sowohl technische als auch nicht-technische Aspekte der Organisationsstruktur. Dazu gehören unter anderem:

- Software-Schwachstellen: Veraltete Software oder fehlende Sicherheitsupdates sind oftmals potenzielle Eintrittspunkte für Angreifer. Schwachstellen in Betriebssystemen, Anwendungen oder Firmware müssen identifiziert und behoben werden, um das Risiko von Angriffen zu minimieren. Ein professionelles Vulnerability- & Patchmanagement ist dafür ein absolutes Muss.
- Physische Sicherheit: Physische Angriffsflächen wie ungesicherte Serverräume, ungeschützte Hardware oder mangelnde Zugangskontrollen können ebenfalls ein erhebliches Risiko darstellen. Unternehmen sollten sicherstellen, dass ihre physische Infrastruktur angemessen geschützt ist, um unbefugten Zugriff zu verhindern.
- Menschliche Fehler: Mitarbeiter können versehentlich oder absichtlich Sicherheitsrichtlinien verletzen und so potenzielle Angriffsflächen schaffen. Schulungen und Sensibilisierungskampagnen sind entscheidend, um das Sicherheitsbewusstsein der Mitarbeiter zu stärken und das Risiko menschlicher Fehler zu minimieren.
- Lieferkettenrisiken: Unternehmen sind zunehmend von ihren Lieferketten abhängig, was neue Angriffsflächen schafft. Schwachstellen bei Lieferanten oder Dienstleistern können sich auf die Sicherheit des gesamten Unternehmens auswirken.

Bewertung und Priorisierung von Risiken

Nach der Identifikation von Angriffsflächen müssen Verantwortliche diese Risiken bewerten und priorisieren. Dabei sollten Faktoren wie die Wahrscheinlichkeit eines Angriffs, die potenziellen Auswirkungen sowie die Verfügbarkeit von Ressourcen für die Risikominderung berücksichtigt werden. Risiken mit einem hohen Schadenspotenzial und einer hohen Eintrittswahrscheinlichkeit sollten prioritär behandelt werden, während diejenigen mit geringerer Bedeutung möglicherweise akzeptiert oder durch Versicherungspolicen abgedeckt werden.

Einführung von Risikominderungsstrategien

Basierend auf der Risikobewertung müssen geeignete Strategien zur Risikominderung entwickelt und implementiert werden. Dazu zählen zusätzliche Sicherheitsmaßnahmen, die Aktualisierung von Richtlinien und Verfahren oder die Umstrukturierung von Prozessen. Deren Wirksamkeit sollte regelmäßig überprüft und angepasst werden.

Sicherheitstechnische Maßnahmen

IMPLEMENTIERUNG EINER SECURITY-STRATEGIE

Die Einrichtung technischer Sicherheitsmaßnahmen ist ein wesentlicher Bestandteil der Cyber-Resilienz, um eigene Systeme und Daten vor potenziellen Bedrohungen zu schützen. Ein strategischer Rahmen, der zunehmend an Bedeutung gewinnt, lautet Zero Trust Security.

Zero Trust Security

Traditionelle Sicherheitsmodelle basieren oft auf dem Prinzip des Vertrauens, bei dem Benutzer und Geräte innerhalb des internen Netzwerks als vertrauenswürdig betrachtet werden. Diese Systeme gelten als überholt, wie die immer größere Anzahl von erfolgreichen Hackerangriffen zeigt. Als moderne Alternative empfehlen Experten das sogenannte Zero Trust Security. Dieser Sicherheitsansatz geht davon aus, dass kein Benutzer, kein Gerät und kein Netzwerkanschluss automatisch vertrauenswürdig ist. Stattdessen wird jeder Zugriffsversuch streng überprüft und autorisiert, unabhängig von seiner Herkunft oder Identität.

Indem Unternehmen Zero Trust-Prinzipien einführen, können sie die Angriffsfläche reduzieren und Kontrolle über den Zugriff auf ihre Systeme und Daten gewinnen. Dies umfasst die Implementierung von Mechanismen wie Micro-Segmentierung, Least-Privilege-Zugriff und kontinuierliche Überwachung und Analyse des Netzwerkverkehrs.

Der Multi Secured Endpoint

Ein Beispiel für eine Technologie, die sich nahtlos in einen Zero-Trust-Sicherheitsrahmen integrieren lässt, ist der <<Multi Secured Endpoint>> Dieser Ansatz des IT-Sicherheitshersteller ESET bietet einen umfassenden Schutz der Endpoints vor einer Vielzahl von Bedrohungen, von Malware und Ransomware bis hin zu Zero-Day-Exploits und gezielten Angriffen.

Mit dem Multi Secured Endpoint legen IT-Verantwortliche einen wichtigen ersten Grundstein für ein sicheres Netzwerk. Im Zusammenspiel vom vorhandenen Malware-Schutz mit einer Festplattenverschlüsselungs- und Multi-Faktor-Authentifizierungslösung sowie Cloud Sandboxing verwandeln Administratoren PCs und Laptops in sogenannte <<gehärtete Endpoints>>. Diese benötigen keine Serverstrukturen oder Verbindungen zum Netzwerk, um optimal gesichert zu sein. Der Multi Secured Endpoint sichert die Devices weit besser ab als andere Systematiken zuvor. Und: Es spielt nun keine Rolle mehr, ob sich das Gerät oder der Anwender im IT-sicheren Bürogebäude befindet. Denn Remote Working wird auch in der Verwaltung zukünftig eine wichtige Rolle spielen.

Detaillierte Informationen zum Thema **Zero Trust Security-Ansatz von ESET** finden Sie in unserer Broschüre.

DAS BESTE FÜR PROPHYLAXE UND FORENSIK: ENDPOINT DETECTION AND RESPONSE (EDR)

Endpoint Detection and Response (EDR) ist eine fortschrittliche Sicherheitstechnologie, die darauf abzielt, verdächtige Aktivitäten an Endpunkten wie Desktops, Laptops und Servern zu erkennen und darauf zu reagieren. Im Gegensatz zu traditionellen Sicherheitslösungen, die sich auf die Erkennung bekannter Malware konzentriert, basiert EDR auf Verhaltensanalysen, maschinellem Lernen und künstlicher Intelligenz, um potenziell schädliche Aktivitäten zu identifizieren, die sich von normalen Benutzerverhalten unterscheiden.

Wie EDR arbeitet:

EDR-Lösungen überwachen kontinuierlich das Verhalten von Endpoints in Echtzeit und analysieren Daten wie Prozessausführungen, Dateiaktivitäten und Netzwerkverbindungen. Durch die Analyse dieser Daten können verdächtige Aktivitäten identifiziert werden, die auf eine mögliche Sicherheitsverletzung hinweisen. EDR-Plattformen verwenden häufig eine Kombination aus Signaturerkennung, maschinellem Lernen und Verhaltensanalysen, um potenzielle Bedrohungen zu erkennen, die von herkömmlichen Sicherheitslösungen möglicherweise übersehen werden.

Darüber hinaus ermöglicht EDR eine schnelle Reaktion auf Sicherheitsvorfälle, indem es automatisierte Reaktionsmechanismen bereitstellt, um verdächtige Aktivitäten zu stoppen, kompromittierte Endpoints zu isolieren und die Ausbreitung von Malware zu verhindern. Dies hilft Unternehmen, die Auswirkungen von Sicherheitsvorfällen zu minimieren und die Wiederherstellungszeit zu verkürzen.

Wie EDR bei forensischer Untersuchung helfen kann:

Im Falle eines Sicherheitsvorfalls spielt EDR eine entscheidende Rolle bei der forensischen Untersuchung, um die Ursachen des Vorfalls zu ermitteln, den Umfang des Angriffs zu verstehen und geeignete Gegenmaßnahmen zu ergreifen. EDR-Lösungen erfassen umfassende Daten über die Aktivitäten an Endpunkten, einschließlich detaillierter Protokolle von Prozessausführungen, Dateiänderungen und Netzwerkverbindungen.

Diese Daten können forensischen Analysten helfen, forensische Indizien zu finden, die den Verlauf des Angriffs rekonstruieren und die Taktiken, Techniken und Verfahren (TTPs) des Angreifers identifizieren. Durch die Analyse dieser Indizien können Sicherheitsteams den Angriff besser verstehen, Schwachstellen identifizieren, die Auswirkungen des Vorfalls abschätzen und Maßnahmen ergreifen, um ähnliche Angriffe in Zukunft zu verhindern.

MANAGED DETECTION AND RESPONSE ALS ALTERNATIVE ZU EDR IN EIGENREGIE

Endpoint Detection and Response-Lösungen (EDR) sind aber nicht für alle KMU praktikabel. Die Implementierung und Wartung solcher Lösungen erfordern erhebliche Ressourcen und Fachkenntnisse, die viele kleinere und mittelgroße Unternehmen eher nicht haben. Doch es gibt eine elegante Lösung: Man betreibt EDR nicht in Eigenregie, sondern überträgt diese Aufgabe an externe Dienstleister. In diesem Fall spricht man von Managed Detection and Response (MDR).

Dahinter verbirgt sich ein Ansatz zur Sicherung von IT-Systemen und Daten vor Cyberbedrohungen. Im Wesentlichen handelt es sich dabei um einen Service, der von spezialisierten Anbietern bereitgestellt wird und eine umfassende Überwachung, Erkennung und Reaktion auf potenzielle Sicherheitsvorfälle umfasst. MDR-Provider nutzen fortschrittliche Technologien wie künstliche Intelligenz, maschinelles Lernen und Verhaltensanalysen, um verdächtige Aktivitäten in Echtzeit zu identifizieren und Maßnahmen einzuleiten.

ESET MDR EIGNET SICH IDEAL FÜR KMU

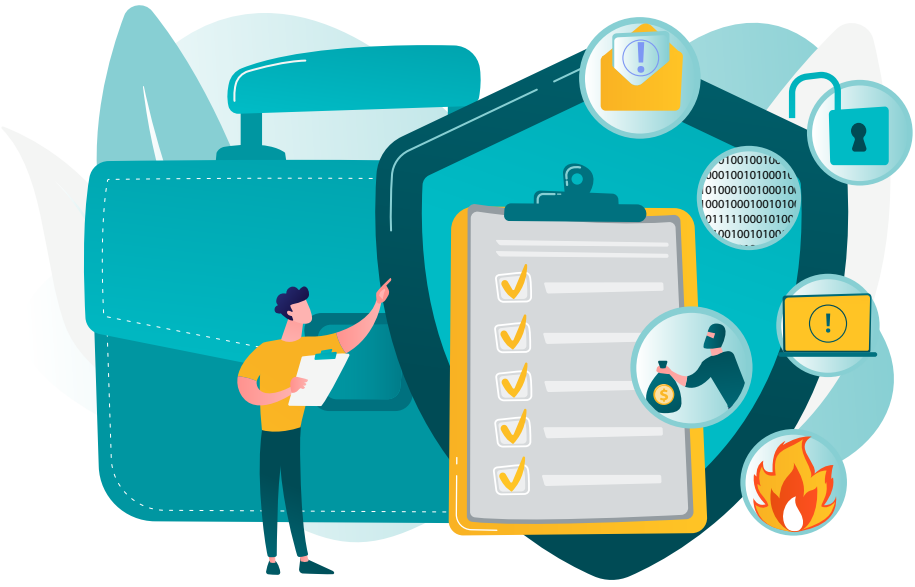
Beispielsweise übernimmt ESET MDR für KMU rund um die Uhr Systemüberwachung, Bedrohungserkennung und -verfolgung, Vorfallreaktion sowie erweiterte Erkennungs- und Reaktionsfunktionen. Dabei handelt es sich um einen KI-basierten Dienst, der das Netzwerk überwacht und prüft. Alle ESET MDR-Kunden sind mit dem ESET eigenen Security Information and Event Management (SIEM) Tool verbunden, sodass Bedrohungen erkannt und mit vordefinierten Reaktionsmaßnahmen gestoppt werden können. ESET MDR ist in der Lage, Bedrohungen innerhalb von 20 Minuten zu erkennen und darauf zu reagieren. Dazu nutzt ESET eigene innovative Cybersicherheitstechnologien und Telemetriedaten, die das Unternehmen weltweit sammelt und auswertet. Für eine effektive Gefahrenabwehr können Kunden zudem auf eine Bibliothek mit vordefinierten Mustern zugreifen und eigene benutzerdefinierte Regeln erstellen. Bei bestimmten Erkennungen oder verdächtigem Verhalten von Dateien oder Prozessen werden dann entsprechende Aktionen ausgelöst.

FAZIT

Selbst mit den besten Sicherheitsvorkehrungen können Cyberangriffe nie zu 100 Prozent verhindert werden. Unternehmen sollten daher einen umfassenden Incident Response Plan entwickeln, der festlegt, wie sie im Falle eines Angriffs reagieren und die Auswirkungen minimieren können. Dieser Plan sollte regelmäßig getestet und aktualisiert werden. Nur so kann man sich sicher sein, dass er im Ernstfall effektiv ist.

#1 Was tun, wenn es knallt

- Trennen Sie die infizierten Systeme vom Netzwerk und vom Internet, um eine weitere Ausbreitung des Angriffs zu verhindern.
- Informieren Sie Ihr IT-Sicherheitsteam oder Ihren IT-Dienstleister, damit sie den Vorfall analysieren und beheben können.
- Dokumentieren Sie alle relevanten Informationen über den Angriff, wie beispielsweise den Zeitpunkt, die Art, die Quelle, die Auswirkungen usw.
- Ändern Sie alle Passwörter für die betroffenen Konten und Systeme, um den Zugriff der Angreifer zu blockieren.
- Benachrichtigen Sie die zuständigen Behörden oder die Polizei und erstatten Sie gegebenenfalls Anzeige.
- Informieren Sie Ihre Kunden, Partner und Mitarbeiter über den Vorfall und die möglichen Folgen für ihre Daten und Dienste.
- Überprüfen Sie Ihre Backups und stellen Sie die Daten und Systeme wieder her, sobald der Angriff beseitigt ist.
- Überprüfen Sie Ihre IT-Sicherheitsmassnahmen und verbessern Sie sie, um künftigen Angriffen vorzubeugen.



Der Unterschied zwischen EDR und MDR

Endpoint Detection and Response (EDR) und Managed Detection and Response (MDR) sind zwei wichtige Ansätze in der IT-Sicherheit. Obwohl sie ähnlich klingen, besitzen sie deutliche Unterschiede.

Endpoint Detection and Response kommt auf Endpoints (z. B. Computer oder Server) zum Einsatz. Die Lösung konzentriert sich darauf, Angriffe auf spezifischen Geräten zu erkennen und einzudämmen. EDR analysiert das Unternehmensnetzwerk anhand von Funktionen wie Bedrohungserkennung, Verhaltensanalyse und Reaktion auf Sicherheitsvorfälle. Endpoint Detection and Response wird in der Regel in Eigenregie der IT-Abteilung betrieben.

Managed Detection and Response ist ein Security-Service, den externe Dienstleister für eine Organisation betreiben. Dies beinhaltet Sicherheitsüberwachung und -management über die gesamte IT-Umgebung des Auftraggebers hinweg. MDR-Anbieter können EDR-Lösungen als Teil ihres Toolkits verwenden: Deswegen ist MDR keine «Entweder-oder»-Entscheidung. Menschen spielen in dieser Dienstleistung eine wichtige Rolle, da sie Echtzeitanalysen durchführen und auf Bedrohungen reagieren können. Kostengünstige MDR-Services ersetzen bereits einen Grossteil der manuellen Aktivitäten durch Künstliche Intelligenz.

Jetzt schon auf NIS2 vorbereiten

Unter dem Motto „Flicken reicht in der IT-Sicherheit nicht aus" hat ESET eine umfassende Kampagne zur NIS2-Richtlinie („Netz- und Informationssicherheitsrichtlinie 2") der Europäischen Union gestartet. Denn viele Organisationen haben sich bisher nur wenig oder gar nicht mit dieser Vorgabe zur Cyber-Security beschäftigt – obwohl sie davon betroffen sein könnten. Ziel der Initiative ist es, Organisationen objektiv zu informieren und Ratschläge für die technische Umsetzung zu geben. Im Zentrum der Kampagne steht die ESET Webseite www.eset.de/nis2. Auf dieser finden Interessierte kostenfrei Whitepaper, Podcasts, Webinare und weitere Informationen rund um das Thema NIS2.

3 VON ÜBER 400.00 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 Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110.000.000+

Geschützte Nutzer weltweit

195+

Länder & Regionen

400.000+

Geschützte Unternehmen

13

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 Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mithilfe 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 allein auf modernste Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

KONTAKTMÖGLICHKEITEN

Sie haben Fragen?
Wir beraten Sie gerne.

JETZT KONTAKT AUFNEHMEN

welivesecurity BY ESET

ESET Digital Security Guide