Cybersecurity-Zertifizierungen: Schlüssel zum beruflichen Erfolg in der IT

Digital Security
Progress. Protected.

ESET.DE | ESET.AT | ESET.CH

Informationssicherheit ist ein breites und dynamisches Fachgebiet in der IT, dass wie viele andere Bereiche eine ständige Beschäftigung mit neuen Entwicklungen erfordert. Deshalb ist für Unternehmen die regelmäßige Weiterbildung ihrer IT-Sicherheitsexperten wichtig. Sie können damit dauerhaft einen hohen Sicherheitsstandard verwirklichen und das Kundenvertrauen steigern. Dies hat letztlich Auswirkungen auf den wirtschaftlichen Erfolg.

Um die Fähigkeiten von Mitarbeitern nachzuweisen, gibt es sogenannte Personenzertifizierungen. Sie bestätigen den Absolventen einer Schulung und der daran anschließenden Prüfung, dass sie bestimmte Kenntnisse in Cybersecurity besitzen. Die Mitarbeiter selbst können damit ihre beruflichen Entwicklungsmöglichkeiten verbessern und sich Chancen auf dem Arbeitsmarkt eröffnen.

Was ist eine Personenzertifizierung?

Cybersecurity-Zertifizierungen für Personen sind in der IT-Branche wichtige Kennzeichen für die Qualifikation einer Fachkraft für IT-Security. Sie dienen dazu, das Fachwissen und die praktischen Fähigkeiten nachzuweisen. Im Regelfall muss die jeweilige Person einen entsprechenden Kurs besuchen und eine standardisierte Prüfung bestehen. Im Anschluss daran erhält die Person ein Zertifikat – eine Urkunde, die das Ergebnis der Prüfung dokumentiert. Allerdings haben die Zertifikate unterschiedliche Gültigkeitsdauern und müssen dann erneuert werden.

Zertifikate sind normalerweise nicht kostenlos. Sowohl für die erste, als auch für alle weiteren Schulungen sowie Prüfungen werden Gebühren fällig. Verbunden mit einem Zertifikat ist die Erlaubnis, eine Bezeichnung wie „Certified Information Systems Security Professional (CISSP)“ oder „Certified Information Security Manager (CISM)“ zu führen. Besitzer des Zertifikates können diese Bezeichnung beispielsweise auf LinkedIn erwähnen, in einen Briefkopf oder eine Visitenkarte einfügen oder auf ihrer eigenen Website damit werben. Dazu gehört nicht nur das Logo, sondern auch eine spezielle, weltweit eindeutige Zertifikatsnummer. Sie ist ein digitaler Nachweis, der auf der Website der Zertifizierungsstelle überprüft werden kann.

Welche Vorteile hat eine Personenzertifizierung?

Der größte Vorteil einer Zertifizierung ist der Nachweis von Fachwissen in einem bestimmten Bereich. Dies ist oft karriereförderlich, da manche Positionen nur auf der Basis von nachweisbaren Kenntnissen vergeben werden. Zudem sind viele Zertifikate international anerkannt, sodass die Chancen auf dem globalen Arbeitsmarkt steigen. Ein weiterer Vorteil: Tendenziell haben zertifizierte Personen ein höheres Gehalt als nicht-zertifizierte.

Doch neben den Karriere-Chancen besitzt der Erwerb eines oder sogar mehrerer Zertifikate im eigenen Arbeitsbereich weitere Vorteile. So hat das Arbeitsfeld Informationstechnologie eine besonders starke Dynamik. Die Geschwindigkeit, in der sich Standards und Best-Practices ändern, ist enorm hoch. Deshalb ist es für IT-Experten – vor allem im Bereich Cybersecurity – sehr sinnvoll, sich kontinuierlich weiterzubilden und aktuelle Entwicklungen zu verfolgen. Der Erwerb von Zertifikaten ist ein motivierender Faktor, da das Wissen mit ihnen dokumentiert wird.

Welche Arten von Personenzertifizierungen gibt es?

Der Markt für Personenzertifizierungen ist schwer zu überblicken. Es gibt viele Security-Zertifizierungen von deutschen und internationalen Anbietern. Das sind unter anderem

- das Bundesamt für Sicherheit in der Informationstechnik (BSI),
- der Bundesverband IT-Sicherheit TeleTrusT,
- der internationale IT-Branchenverband CompTIA,
- die Information Systems Audit and Control Association (ISACA) und
- das International Information System Security Certification Consortium (ISC)².

Darüber hinaus gibt es Hersteller-Zertifikate mit Cybersecurity-Schwerpunkt, beispielsweise von Microsoft, Cisco, AWS oder IBM. Diese Zertifizierungen sind stärker spezialisiert und fokussieren sich ausschließlich auf Security-Aspekte der Lösungen der jeweiligen Hersteller.

Welche deutschen Zertifizierungen sind im Arbeitsmarkt relevant?

Für Personenzertifizierungen gibt es unterschiedliche Zielgruppen und Zertifizierungsbereiche. Deshalb begrenzt sich dieser Beitrag auf wichtige Zertifizierungen für IT-Fachkräfte in Unternehmen.

Zusätzlich gibt es auch Personenzertifizierungen, die nur in Behörden oder Zertifizierungsstellen relevant sind. Sie sind hier ebenso wenig berücksichtigt wie reine Hersteller-Zertifizierungen. Es ist sicher sinnvoll, eine Qualifikation für Security bei bestimmten IT-Lösungen nachzuweisen. Doch eine solche Zertifizierung ist eher als Zusatzqualifikation zu sehen, die eine der hier vorgestellten allgemeinen Security-Zertifizierungen ergänzt.

Die Zertifizierung des TeleTrusT

Der Bundesverband IT-Sicherheit TeleTrusT bietet ein EU-weit geltendes Personenzertifikat für den Bereich Informationssicherheit. Es ist anders als internationale Zertifikate besonders auf europäische Standards zugeschnitten, zum Beispiel auf spezifische Haftungsregelungen, den europäischen Datenschutz sowie nur in einzelnen Ländern geltende Regeln.

Die Zertifizierung berechtigt zum Führen des Titels TeleTrusT Information Security Professional. Zur Prüfungsvorbereitung gibt es bei zahlreichen lizenzierten Anbietern Schulungen, darunter einige kommerzielle Anbieter, aber auch das Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt. Die Prüfung selbst ist beim Unternehmen PersCert TÜV, einem Teil der TÜV Rheinland Gruppe.

Das Spektrum der Inhalte von Schulungen und Prüfungen ist sehr breit und stark praxisorientiert. Unter anderem geht es um Themen wie Betriebssystemsicherheit, Netzwerksicherheit, mobile Endgeräte, Kryptographie, ISO 27001 und vieles mehr. Die Zertifizierung setzt damit ein umfassendes Wissen über Informationssicherheit sowie die deutsche und europäische Gesetzgebung zur Cybersecurity voraus. Für die Teilnahme wird eine mindestens dreijährige Berufserfahrung mit entsprechenden Referenzen erwartet.

Die Zertifizierungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet viele Zertifizierungen für Produkte, Unternehmen und Personen. Ein Überblick darüber findet sich auf der Website der Behörde. Für Cybersecurity-Experten in Unternehmen sind drei Zertifizierungen relevant.

- IT-Grundschutz-Berater: Sie begleiten und unterstützen Unternehmen bei der Einführung eines Managementsystems zur Informationssicherheit, das auf dem IT-Grundschutzkatalog des BSI basiert. Für diese Zertifizierung gibt es eine spezielle Weiterbildung, die zweistufig organisiert ist. Der erste Schritt ist die Prüfung als IT-Grundschutz-Praktiker, erst der zweite Schritt führt zur Zertifizierung als Berater. Die entsprechenden Schulungen gibt es bei zahlreichen Schulungsanbietern. Die Prüfung und Zertifizierung selbst findet nur beim BSI statt. Wichtig: Teilnehmen kann nur eine Person mit abgeschlossener Berufsausbildung, achtjähriger Berufserfahrung sowie dreijähriger Beteiligung an entsprechenden Beratungsprojekten.

- Vorfall-Experten: Sie unterstützen Einzelpersonen sowie kleine und mittelgroße Unternehmen bei der Bearbeitung von Sicherheitsvorfällen. Ihre Aufgabe: Schäden eindämmen, Ursachen ermitteln und Systeme wiederherstellen. Um sich zertifizieren zu

lassen, müssen die Experten die gleichen beruflichen Voraussetzungen wie ein angehender IT-Grundschutz-Berater haben und darüber hinaus eine leitende Position im Bereich Informationssicherheit und Vorfallbehandlung nachweisen können. Für die Prüfungsvorbereitung gibt es dreitägige Weiterbildungen bei zahlreichen Schulungsanbietern. Die Prüfung kann nur beim BSI abgelegt werden.

- IS-Penetrationstester: Bei dieser Testform werden Angriffe simuliert, um die Sicherheit von Computersystemen überprüfen – ein gängiges Verfahren in der Cybersecurity. Erfahrene Tester können sich vom BSI zertifizieren lassen. Voraussetzung dafür ist eine Anstellung bei einem vom BSI zertifizierten IT-Sicherheitsdienstleister. Außerdem werden mindestens zwei Jahre Berufserfahrung mit 100 Projekttagen bei der Überprüfung von Computersystemen vorausgesetzt. Eine alternative Qualifikation ist ein Jahr Berufserfahrung mit entsprechenden Fortbildungen.

Besonders empfehlenswert ist die Zertifizierung als IT-Grundschutz-Berater. Sowohl angestellte als auch selbständige Sicherheitsexperten können davon stark profitieren. Sinnvoll ist sie erstens für Mitarbeitende in Unternehmen, die sich nach IT-Grundschutz (ISO 27001) zertifizieren lassen möchten und zweitens für Mitarbeitende in IT-Unternehmen, die Mittelständler bei der Einführung von IT-Grundschutz beraten.

Welche internationalen Zertifizierungen sind relevant?

Die bisher vorgestellten Zertifizierungen sind entweder stark auf den deutschen Markt ausgerichtet oder gelten (nur) europaweit. Es gibt allerdings auch Personenzertifizierungen für Cybersecurity, die weltweit gelten. Sie werden von internationalen Unternehmen auch in Europa häufiger gefordert.

Die CompTIA-Zertifizierungen

Die Computing Technology Industry Association (CompTIA) ist ein internationaler Branchenverband der IT-Industrie. Zu den Mitgliedern zählen Unternehmen, Selbstständige und andere Branchenangehörige aus mehr als 100 Staaten der Welt. Eines der wichtigsten Ziele des Verbandes ist die Schaffung von einheitlichen Standards bei der Aus- und Weiterbildung von IT-Fachkräften. Hierfür bietet der Verband herstellerneutrale IT-Zertifizierungen an, unter anderem auch für Cybersecurity.

Insgesamt gibt es vier aufeinander aufbauende Personenzertifizierungen für Cybersecurity. Entsprechende Schulungen gibt es von zahlreichen Anbietern, sowohl als Präsenz-wie auch als Online-Schulung. Darüber hinaus gibt es zahlreiche Lehrmaterialien für dasselbe Studium. Die eigentliche Zertifizierungen geschieht an den Standorten des Unternehmens Pearson VUE.

- CompTIA Security+: Wer dieses Zertifikat besitzt, zeigt damit grundlegende Kenntnisse im Bereich der Cybersecurity. Voraussetzungen ist eine zweijährige Berufserfahrung in IT-Security. Inhaltlich geht es hier um generelle Sicherheitskonzepte für Zugangskontrolle, Authentifizierung und Angriffsabwehr sowie um Expertise bei Netzwerk- und Infrastruktursicherheit sowieso in den Grundlagen der Verschlüsselung.

- CompTIA CySA+: (Cybersecurity Analyst): Bei dieser Zertifizierung geht es hauptsächlich um Verhaltensanalysen an Netzwerken und Geräten. Thema der Schulungen sind aktuelle Methoden und Tools wie beispielsweise Threat Intelligence, Security Information and Event Management (SIEM) oder Endpoint Detection and Response (EDR). Voraussetzung für die Teilnahme an der Prüfung sind mindestens vier Jahre praktische Erfahrung in der Informationssicherheit.

- CompTIA CASP+: (Advanced Security Practitioner): Dieses Zertifikat richtet sich an fortgeschrittene Security-Spezialisten und beschäftigt sich mit Themen wie Risikomanagement, Sicherheitsarchitekturen, Informationssicherheits-Managementsysteme sowie die technische Integration von Security-Maßnahmen. Voraussetzung für die sehr praxisorientierte Prüfung sind zehn Jahre Erfahrung in der IT-Administration, davon fünf Jahre praktische Erfahrung im Bereich der technischen Sicherheit.

- CompTIA PenTest+: Mit diesem Zertifikat können Cybersecurity-Spezialisten ihre Fähigkeiten beim Penetration Testing und dem Schwachstellenmanagement nachweisen. Voraussetzung für die Teilnahme sind mindestens drei Jahre praktische Erfahrungen der Informationssicherheit.

- Die Zertifizierungen gelten für drei Jahre und müssen anschließend neu geprüft werden. Eine Rezertifizierung wird etwas einfacher, wenn die Absolventen an dem Continuing Education (CE)-Programm von CompTIA teilnehmen. In diesem Fall müssen sie innerhalb dieser drei Jahre 75 Continuing Education Units (CEUs) nachweisen. Dafür eignen sich alle Schulungen, die sich auf den Inhalt der Zertifikate beziehen.

Die internationalen ISACA-Zertifizierungen

Die ISACA (Information Systems Audit and Control Association) ist ein unabhängiger, globaler Berufsverband für IT-Revisoren, Wirtschaftsprüfer sowie Experten der Informationssicherheit und IT-Governance. Sie bietet eine Vielzahl an Zertifizierungen an, die teils international, teils nur für Deutschland gelten. Drei Zertifizierungen der ISACA sind weltweit anerkannt und eignen sich für den Nachweis von Fachwissen rund um Cybersecurity:

- Certified Information Security Manager (CISM): Die Zertifizierung richtet sich an erfahrene Führungs- und Fachkräfte auf dem Gebiet der IT-Security. Sie können damit ihre Qualifikation für Planung, Umsetzung, Steuerung und Überwachung von Security-Konzepten nachweisen. Das Examen richtet sich an Experten mit mindestens fünf Jahren nachweisbarer Berufserfahrung bei der aktiven Gestaltung der Informationssicherheit in einem Unternehmen. Inhaltlich geht es um Governance, Risikomanagement, Security-Programme und Incidentmanagement.

- Certified in Risk and Information Systems Control (CRISC): Diese Zertifizierung hilft Security-Experten, sich auf dem Gebiet des IT- und Enterprise-Risikomanagement weiterzubilden. Erforderlich ist eine nachweisliche, fundierte Berufserfahrung von drei oder mehr Jahren in Risikomanagement und interne Kontrolle im IT-Umfeld. Inhaltlich geht es hier um Governance, Risikobewertung, Risikobehandlung und -berichterstattung sowie Informationssicherheit.

- Information Security Practitioner (ISP): Diese Zertifizierung richtet sich auf wesentliche Aspekte der Informationssicherheit in Unternehmen und der Nutzung von Informationssicherheit-Management System. Zur Zielgruppe gehören Berater und Auditoren mit Schwerpunkt Informationssicherheit sowieso Informationssicherheitsbeauftragte in Unternehmen. Das Zertifikat eignet sich auch für Berufsanfänger.

Ein wichtiger Hinweis: Für die ISACA-Zertifizierungen CISM und CRISC gilt eine Weiterbildungspflicht. Sie wird über sogenannte CPE-Punkte (Continuing Professional Education) nachgewiesen. Die Träger der Zertifizierung müssen innerhalb von drei Jahren mindestens 120 CPE-Punkte nachweisen, die bei einer Zertifizierungsstelle gemeldet werden müssen. Hierfür sind Schulungen mit Vergabe von CPE-Punkten notwendig, die es allerdings nicht bei jedem Anbieter gibt. Wer seiner Weiterbildungspflicht genügen will, kann auch zusätzliche Zertifikate mit Vergabe von CPE-Punkten erwerben, etwa beim German Chapter.

Die ISACA-Zertifizierungen für Deutschland

Einige Zertifizierungen gelten nur in Deutschland und sind vom Germany Chapter der ISACA zusammen mit dem BSI und einem Schulungsanbieter entwickelt worden. Sie bestehen aus drei aufeinander aufbauenden Kursen sowie den jeweiligen Zertifizierungen.

- Cyber Security Grundlagen (CSG): Das Zertifikat bescheinigt den Absolventen einen Überblick über aktuelle, technische Schutz- und Überwachungsmaßnahmen im Bereich der Cybersecurity. Es richtet sich an Personen mit IT-Grundkenntnissen.

- Cyber Security Practitioner (CSP): Das Zertifikat bescheinigt Kenntnisse über wesentliche Aspekte der Cybersicherheit sowie der Prinzipien und Vorgehensweisen für Sicherheitsprüfungen. Das Zertifikat gilt für drei Jahre. Es kann verlängert werden, wenn sechs Cybersecurity-Checks oder ähnlich Prüfungen nachgewiesen werden.

- Cyber Security Expert (CSE): Aufbauend auf den beiden anderen Zertifizierungen geht es hier um Verfahren zur Erkennung und Bewältigung von Cyberangriffen. Dabei wird besonders viel Wert auf Praxis gelegt. Die Teilnehmer der entsprechenden Kurse erhalten zum Abschluss die Aufgabe, einen Live-Angriff auf eine simulierte IT-Umgebung zu erkennen und abzuwehren.

Diese Schulungen bieten eine einheitliche berufliche Qualifizierung und werden ausschließlich von der ISACA angeboten. Die Teilnehmer erhalten CPE-Punkte.

Die (ISC)²-Zertifizierungen

Das International Information System Security Certification Consortium (ISC)² ist eine gemeinnützige Organisation, die Schulungen und Zertifizierungen für Cybersicherheit anbietet. Dafür definiert es einen sogenannten Common Body of Knowledge (CBK), der glob noch lebe ale Industriestandards und Best-Practices der Informationssicherheit definiert. Dazu gehören die folgenden Wissensgebiete:

1. Security And Risk Management

2. Asset Security

3. Security Architecture And Engineering

4. Communication And Network Security

5. Identity And Access Management (IAM)

6. Security Assessment And Testing

7. Security Operations

8. Software Development Security

Die wichtigste Zertifizierung des (ISC)² erinnert eher an einen Universitätsabschluss als an ein IT-Zertifikat. Sie dürfte allerdings auch auf dem Arbeitsmarkt den größten Wert haben: Der Certified Information Systems Security Professional (CISSP). Diese Zertifizierung gehört zu den renommiertesten, die es im Bereich der Informationssicherheit gibt. Sie ist in Großbritannien einem Master of Science gleichgestellt. Die Zertifizierung gilt für einen Zeitraum von sechs Jahren und ist vor allem geeignet für Security-Berater, Sicherheitsarchitekten sowie Security-Experten, die eine Rolle als Chief Information Security Officer (CISO) anstreben.

Das CISSP-Zertifikat richtet sich an erfahrene Sicherheitsexperten, die mindestens fünf Jahre Erfahrung in zwei der acht Wissensgebiete des CBK haben. Ein Hochschulabschluss in Informationssicherheit oder eine andere Zertifizierung senken diese Frist um ein Jahr. Eine Besonderheit, die diese Zertifizierung von den anderen abhebt: Die Qualifikation der Person muss zusätzlich zur bestandenen Prüfung von einer anderen zertifizierten Person bestätigt werden.

Grundsätzlich können auch Personen ohne fünf Jahre Berufserfahrung die Prüfung ablegen und damit den Titel „Associate of (ISC)²" erwerben. Beim Nachweis der notwendigen Berufserfahrung vor Ablauf der Zertifizierung wird das CISSP-Zertifikat verliehen. Im Anschluss kann die zertifizierten Person eine Spezialisierung in den Bereichen Architektur, Engineering und Management anstreben. Hierfür gibt es drei zusätzliche Zertifizierungen.

Ähnlich wie bei den ISACA-Zertifizierungen gibt es auch beim (ISC)² eine Weiterbildungspflicht. Für den Erhalt der CISSP-Zertifizierung müssen die Kandidaten alle drei Jahre mindestens 120 CPE-Punkte (Continuing Professional Education) erwerben und zwar in jedem Jahr mindestens 40 Punkte.

Neben diesem umfangreichen Zertifizierungsprozess gibt es noch zwei weitere Zertifizierungen mit einem etwas engeren Fokus. Sie richten sich in erster Linie an Praktiker aus dem IT-Betrieb bzw. der Anwendungsentwicklung:

- Certified Secure Software Lifecycle Professional (CSSLP): Diese Zertifizierung richtet sich an Security-Experten mit mindestens vier Jahren Erfahrung im Software-Lebenszyklus (SDLC). Die Zertifizierung bescheinigt fortgeschrittene technische Fähigkeiten für die Entwicklung, Verwaltung und Pflege von sichererer Software.

- Certified Cloud Security Professional (CCSP): Diese Zertifizierung richtet sich an IT-Fachkräfte mit mindestens fünf Jahren Berufserfahrung, von denen mindestens drei Jahre im Bereich der Informationssicherheit liegen sollten. Die Zertifizierung bescheinigt Fähigkeiten in den Bereichen Cloud-Infrastruktur, -Design sowie -Security.

Was kosten Zertifizierungen?

Vor allem für die renommierten, internationalen Zertifizierungen mit Weiterbildungspflichten entstehen unter Umständen Kosten im vierstelligen Bereich. Zahlen müssen die Prüflinge für die entsprechenden Schulungen und die eigentliche Prüfung sowie für die

Seminare, die für eine Rezertifizierungen notwendig sind. Unter Umständen entstehen auch weitere Kosten, beispielsweise für Schulungsmaterial, Online-Kurse und Fachbücher oder Fahrt-, Übernachtungs- und Verpflegungskosten für Präsenzschulungen.

Wer bezahlt die Zertifizierungen?

Bei angestellten IT-Experten übernimmt meist der Arbeitgeber die Kosten. Die Voraussetzung: Die Zertifizierung dient der Weiterbildung für den aktuellen oder einen angestrebten Arbeitsbereich. Die Übernahme von weiteren Kosten etwa für Fachbücher und anderen Schulungsmaterial kann oft ebenfalls mit dem Arbeitgeber vereinbart werden. Genaue Informationen gibt es bei der Personalabteilung oder dem Betriebsrat.

Sind Zertifizierungen steuerlich anrechenbar?

Sofern der Arbeitgeber die Kosten nicht übernimmt, sind sämtliche Ausgaben für die berufliche Fortbildung steuerlich in unbegrenzter Höhe als Werbungskosten anrechenbar. Dazu gehören Fachseminare, Fachtagungen, Kongresse, Schulungsmaterialien und Fachbücher sowie die Kosten für Prüfungen und Zertifizierungen inklusive der Fahrtkosten sowie der Übernachtung- und Reisenebenkosten. Deshalb ist es für einen Angestellten sinnvoll, sämtliche Belege rund um die Fortbildung aufzubewahren und bei der Steuererklärung beizulegen. Genaue Informationen gibt es bei einem Steuerberater.

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.

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

ISO 9001 SGS

ISO/IEC 27001 SGS

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

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