ROHDE&SCHWARZ
Make ideas real

Rohde&Schwarz Cybersecurity

ONLINEZUGANGSGESETZ & DATENSCHUTZ: MIT SICHERHEIT ZUR DIGITALEN BEHÖRDE

Schließen Sie versteckte Sicherheitslücken mit R&S®Web Application Firewall

INHALT

1 DIGITALER WANDEL: DIE LÜCKE SCHLIEßEN ZWISCHEN WIRTSCHAFT UND ÖFFENTLICHEM SEKTOR

Digitalisierung ist keine Zukunftsvision, sondern ein Fakt.
Doch wie sieht es mit der Digitalisierung in Behörden und der Verwaltung aus?

Bürger*innen in Deutschland bewegen sich mit einer hohen Selbstverständlichkeit in der digitalen Welt und wollen Aktivitäten wie das Beantragen des Personalausweises, Reisepasses, Geburtsurkunden etc. nicht mehr vor Ort im Bürgeramt vornehmen, sondern bequem von zu Hause über den PC oder das Smartphone erledigen. Hier ist der Staat gefordert: In 2017 ist deswegen das Onlinezugangsgesetz (kurz OZG) in Kraft getreten, ein entscheidender Schritt, um die Lücke zwischen den Entwicklungen im privaten und öffentlichen Sektor zu schließen.

Keine Zukunftsvision:
Den Reisepass bequem von zu Hause über den PC beantragen.

2 DIE RAHMENBEDINGUNGEN DES OZG

Das Onlinezugangsgesetz[1] wurde am 14. August 2017 als Art. 9 des „Gesetzes zur Neuregelung des bundesstaatlichen Finanzausgleichssystems“ erlassen[2] und ist am 18. August 2017 in Kraft getreten. Es verpflichtet Bund und Länder, dass bis 2022 alle Verwaltungsleistungen online zur Verfügung stehen müssen. Das gilt für Bund, Länder sowie Kommunen und umfasst insgesamt 575 Einzelleistungen:

Dazu gehören unter anderem auf **Länder- und kommunaler Ebene:**

- KFZ-Zulassungen
- Beantragung der Fahrerlaubnis
- Umzugsmeldungen
- Beantragung der Geburtsurkunde

und auf Bundesebene:

- Beantragung von Arbeitslosen, Wohn- oder Kindergeld
- Anforderung Führungszeugnis
- Prüfung auf Rentenanspruch, Einsehen des Rentenverlaufs und Rentenpunkte

©www.unsplash.com - Massimo Virgilio

Bundestag schafft Rahmenbedingungen:

Das Onlinezugangsgesetz umfasst insgesamt 575 Einzelleistungen.

[1] Langtitel: Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen

[2] Bundesgesetzblatt Teil I Nr. 57, unter: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3122.pdf (abgerufen am 22.04.2020)

3 DIE HERAUSFORDERUNGEN BEI DER UMSETZUNG

Die Angelegenheit ist hochkomplex, da die Verwaltung in Deutschland föderal organisiert ist. „Jedes Bundesland hat eigene Kompetenzen bei der Gesetzgebung. Der Föderalismus unterstützt einerseits die Vielfalt und stärkt die Autonomie der Länder. Andererseits gibt es auch eine Vielzahl parallel existierender Gesetze, Leistungen und Digitalportale. Außerdem besitzen Länder und Kommunen oft nicht die Ressourcen, Digitalisierungsvorhaben und -projekte alleine zu stemmen.“[3] Die Umsetzung muss also auf Bundesebene und dann noch auf Landes- und kommunaler Ebene erfolgen. Dafür gibt es als zentrales Gremium den **IT-Planungsrat**, der das Digitalisierungsprogramm föderal betreut.

Die einzige Vorgabe ist demnach das Gesetz, der entsprechende Prozess bzw. die optimale föderale IT-Architektur muss für die verschiedenen Ebenen erst erarbeitet werden und sich letztendlich dann aber auch in der Praxis bewähren. Dafür wurde die **Föderale IT Kooperation – kurz FITKO** – etabliert.

3.1 Die Digitalisierung und die Sicherheit: Eine Geschichte voller Missverständnisse und Versäumnisse

Das Ausmaß der Herausforderung lässt sich gut an dem Ende des Supports von Microsoft® Windows 7™ illustrieren – „End of Life“ war der 14. Januar 2020. Aber Anfang 2020 gab es noch mindestens 33.000 Rechner auf Bundesebene, die kein Update auf Windows 10™ erfahren haben. „Das Problem findet sich in den Landesverwaltungen wieder. In der Berliner Verwaltung laufen etwa noch rund 20.000 der insgesamt 85.000 Rechner mit Windows 7™.“[4]

Das **größte Problem ist die Sicherheit** – da es hier keinen Support mehr gibt, sind auch keine entsprechenden Sicherheits-Patches mehr verfügbar. Ein großes Einfallstor für Schadsoftware und ein gutes Beispiel dafür, wie das Ausrollen von Prozessen im digitalen Bereich gerade mit Hinblick auf die Sicherheit große Lücken offenbart.

---

[3] Was ist das Onlinezugangsgesetz (OZG)?, unter: Onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-ozg-node.html (abgerufen am: 22.04.2020)

[4] Bielawa, Helen: Frist verpasst: Bund zahlt 800.000 Euro für verlängerten Windows-7-Support, unter: https://t3n.de/news/frist-verpasst-bund-zahlt-euro-1244332/ (abgerufen am 22.04.2020)

Der Bürger fordert zu Recht digitale Prozesse ein, da sie nun in allen anderen Bereichen einen integralen Bestandteil des modernen Alltags darstellen. Doch genauso wollen Bürger*innen die Gewissheit haben, dass die eigenen Daten sicher sind.

In 2019 und in 2020 machten spektakuläre Angriffe auf staatliche Einrichtungen von sich reden. Immer häufiger verschaffen sich Hacker Zugriff auf Daten von Ämtern und Behörden. **Persönliche Daten sind im Darknet sehr gefragt** und lassen sich gut monetarisieren. Diese können von weiteren Tätergruppen für Angriffe genutzt werden. Mit sensiblen, persönlichen Informationen wie Name, E-Mail-Adresse und Kreditkarteninformationen können Onlineaccounts leicht gehackt werden. Gleichzeitig können sensible persönliche Daten zur Erpressung genutzt werden. Kurzum: Der **Hack von Daten ist der Bankraub** des 21. Jahrhunderts. Der Vorteil für Kriminelle: Er ist deutlich einfacher, bedeutet weniger Aufwand und ist zusammengenommen deutlich lukrativer.

Für staatliche Behörden sind extensive Datenhacks ein klarer Vertrauensverlust und im weiteren Sinne auch demokratiegefährdend, denn die Demokratie basiert auf dem Grundvertrauen in die staatlichen Stellen. Demnach ist das Thema Cybersicherheit das Fundament für den digitalen Wandel der staatlichen Behörden und wegweisend in dem Prozess der Umsetzung des Onlinezugangsgesetzes.

4 IST DAS DIGITALE ICH SICHER?

In den verschiedenen Anforderungen an die Umsetzung des OZGs wird darauf hingewiesen, dass durch die Ende-zu-Ende-Verschlüsselung und die Zwei-Faktor-Authentifizierung durch den elektronischen Personalausweis für Sicherheit gesorgt wird. Das betrifft dann aber erst mal nur den Übertragungsweg der Daten und das Identitätsmanagement.

Wenn alle Leistungen online zur Verfügung stehen sollen, dann hat man es mit **Webapplikationen bzw. Webanwendungen**[5] zu tun. Hier muss man sich entweder mit seinem Personalausweis identifizieren oder via Webformular und eines Logins, indem man nach der Erstellung eines Kontos seinen Benutzernamen und das entsprechende Passwort eingibt. Wenn man sich mit dem Personalausweis identifizieren möchte, dann müssen die verschiedenen Portale **Schnittstellen, sogenannte APIs**, zur Verfügung stellen. Dadurch ergeben sich verschiedenen Gefahrenquellen, die mitunter nicht bedacht werden.

Webformulare bzw. Login-Masken[6] sind beliebte Angriffsziele. Damit wird versucht, auf die hinter den Formularen liegenden Daten zu kommen – diese befinden sich in Onlinedatenbanken auf einem Webserver.

Vorsicht ist geboten:
Webformulare können auf verschiedene Arten angegriffen werden.

[5] Streng genommen ist das WWW eine Anwendung im Internet. Das WWW wurde Anfang der 90er von Robert Cailliau und Tim Berners-Lee im europäischen Kernforschungszentrum CERN eingeführt.

[6] Zusatzinformation: Aktuell ist es noch so, dass die Authentifizierung mit dem Personalausweis noch nicht bei allen Anwendungen möglich ist.

WAS IST EINE WEB-APP / WEBANWENDUNG?

Eine Web Application ist eine Anwendung auf einem Webserver, die über einen Webclient in Form eines Browsers wie Internet Explorer, Firefox, Chrome etc. aufgerufen werden kann. Die beiden kommunizieren über Standardprotokolle wie HTTP, FTP oder WebSocket. Hauptsächlich kommunizieren Webserver und Webclients über das HTTP(S)-Protokoll. Der Client fordert auf dem Webserver eine Ressource an, wie z. B. eine in HTML programmierte Webseite. Zwischen Client und Server wird eine Session aufgebaut, die sich aus Request und Response zusammensetzt. Zusammengefasst kann man sagen, dass eine Web-App eine nicht statische Website ist, die komplexe Aufgaben erfüllt. Dazu gehören aus dem privaten Umfeld Facebook, E-Mail-Dienste wie GMX oder Yahoo und aus dem Berufskontext z. B. Skype for Business, Outlook Exchange (OWA) oder SAP-Anwendungen wie die Buchung von Geschäftsreisen von Mitarbeitern.

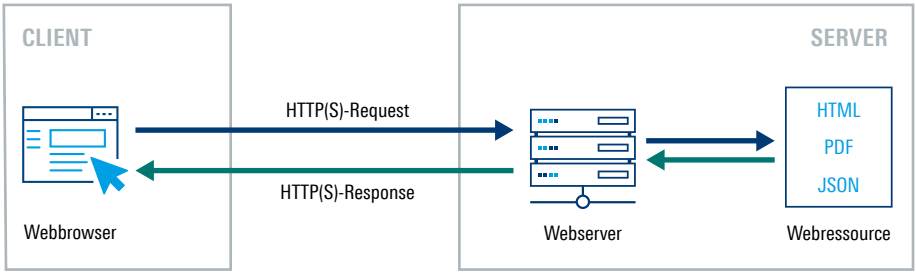

Abbildung 1: Datenfluss bei einer Client-Server-Webanwendung

4.1 Angriffspunkt: Webformulare

Die Top-3-Angriffsarten sind **Injections, Broken Authentications und Sensitive Data Exposure**. Diese gehören zu einer Liste von insgesamt 10 Angriffsarten, die von dem Open Web Application Security Project (OWASP) veröffentlicht wurden. Das ist eine internationale gemeinnützige Organisation, die sich der Sicherheit von Webanwendungen widmet. Eines der Kernprinzipien von OWASP ist, die Sicherheit von Webanwendungen zu verbessern. Dazu gehört die OWASP Top 10.

Hinzu kommen sogenannte „HTTP Floods“ und eine Angriffsart namens Slowloris.

Falls Sie mehr erfahren wollen, ist **hier*** die OWASP Top 10-Liste zu finden.

* https://owasp.org/www-project-top-ten/

Top 1: Injections

Noch immer können Angreifer viel zu häufig mit sogenannten SQL[7]-Befehlen in Webformularen Daten stehlen, wie zum Beispiel Namen, E-Mail-Adressen und Passwörter.

Angreifer „injizieren" bösartigen Code in die Formularfelder, um damit die gesamten Daten zu stehlen, die auf dem Webserver liegen. In der Folge werden diese Daten im Darknet angeboten, um diese Daten für Angriffe z. B. auf Onlinebankingkonten, Amazon-Accounts etc. zu nutzen.

Top 2: Broken Authentication

Mittels dieser Attacke ist der Angreifer in der Lage, sich in die Webanwendung einzuschleichen, ohne sich ordnungsgemäß zu authentifizieren. Das ist mit diesen Maßnahmen möglich:

1. „CREDENTIAL STUFFING":
Der Angreifer hat Benutzernamen und Passwörter und verwendet sie in der Webanwendung mit einem automatisierten Tool.

2. AUTOMATISIERTE ANGRIFFE:
Zufällige Benutzernamen und Passwörter einsetzen, die man zuvor über einen illegalen Weg erworben hat.

3. STANDARDPASSWÖRTER AUSPROBIEREN:
Zum Beispiel Benutzername: admin Passwort: admin oder Benutzername: admin Passwort: passwort. Oft werden diese Default-Einstellungen nicht angepasst.

4. WIEDERHERGESTELLTE SESSION-ID IM GEÖFFNETEN BROWSER AN EINEM ÖFFENTLICHEN TERMINAL PC:
Der Angreifer nutzt eine noch valide Session-ID, die noch im Browser gespeichert ist, öffnet ein neues Tab und bekommt erneut Zugriff auf die Webanwendung.

[7] SQL = Structured Query Language ist die häufigste Sprache, mit der man mit Datenbanken kommuniziert. Deswegen konzentrieren sich die meisten Injection-Angriffe auf diese Sprache.

Top 3: Sensitive Data Exposure

„Sensitive Data Exposure“ war in der OWASP-Top-10-Liste von 2013 noch auf Platz 6 zu finden. In 2019 ist es auf den Platz 3 vorgerückt. Eine passende deutsche Übersetzung wäre „ungenügende Kryptografie gespeicherter und transportierter, wichtiger Daten“ – wie Kreditkarten, Passwörter und beispielsweise Session Identifier.

1. UNZUREICHENDE VERSCHLÜSSELUNG DURCH SCHWACHE CHIFFREN:
Verschlüsselte Daten auf z. B. TLS-verschlüsselten Websites werden von Angreifern auf das unverschlüsselte HTTP heruntergezwungen – dadurch werden sensible Daten offengelegt.

2. VERSCHLÜSSELTE DATEIEN WIE KREDITKARTENNUMMERN/ SOZIALVERSICHERUNGSNUMMERN WERDEN GESTOHLEN:
Diese lassen sich durch systematisches Durchprobieren, z. B. mit Wortlisten oder sogenannten Regenbogentabellen („Rainbow Tables“: bekannte Liste von Passwörtern) zum Teil leicht entschlüsseln.

Weitere Angriffe – HTTP Flood, Slowloris

HTTP Floods und Slowloris sind Varianten von DDoS[8]-Angriffen: Sie scheinen legitime Anfragen über das HTTP-Protokoll an den Webserver zu stellen, legen aber letztendlich durch eine Vielzahl von Anfragen durch Botnetzwerke den Webserver lahm. Die verschiedenen Onlinedienste sind in der Folge nicht mehr erreichbar.

[8] DDoS-Angriff: Distributed Denial of Service Angriff, mit dem durch eine Vielzahl von bösartigen HTTP-Befehlen der gesamte Web Server lahm gelegt wird.

4.2 Angriffspunkt: APIs (Application Programming Interfaces)

In Sachen Authentifizierung ist mit dem elektronischen Personalausweis schon ein großer Schritt nach vorne gemacht. Laut verschiedener Experten ist dieser auch erst mal sicher vor möglichen Manipulationen.

Aber was an der Stelle übersehen wird, sind die verschiedenen Schnittstellen – besser bekannt als APIs oder Application Programming Interfaces – der Verwaltungsportale, die dem Personalausweis zur Identifizierung anderen mobilen Apps oder Informationssystemen zum Informationsaustausch zur Verfügung gestellt werden. Diese APIs sind heute die Schlüsselkomponenten bei der Entwicklung digitaler Lösungen. Sie machen 80 % des HTTP-Verkehrs aus. Sie gelten heute als die größte Sicherheitslücke. Aus diesem Grund gibt es bereits eine spezielle OWASP-API-Liste mit den 10 wichtigsten Angriffstypen.

Hier* finden Sie die aktuelle OWASP API Top 10-Liste und ein **Rohde & Schwarz-Webinar**** zu dem Thema.

WAS SIND APIs?

Über APIs werden Ressourcen und Dienste in Form von Schnittstellen für andere Anwendungen verfügbar gemacht. Bedauerlicherweise stellt jede API jedoch auch ein Risiko im Hinblick auf Sicherheit und Compliance dar. Diesem Risiko muss begegnet werden, um die durch APIs übermittelten Informationen zu schützen. Ungeschützte APIs können zur Kompromittierung von Kunden- und Bürgerdaten oder Backend-Servergeräten führen und den Zugriff auf Daten durch Unbefugte ermöglichen.

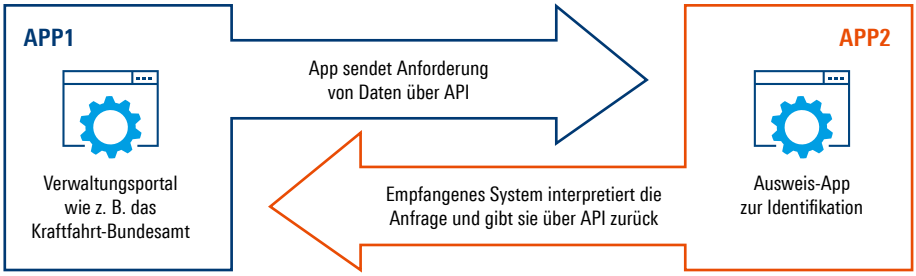

Abbildung 2: Datenaustausch zwei verschiedener Apps

* https://owasp.org/www-project-api-security/
** https://www.youtube.com/watch?v=MH9aETEgrQQ

5 WEB APPLICATION FIREWALL: MIT SICHERHEIT ZUR DIGITALEN BEHÖRDE

Zu all den genannten Angriffen ist festzuhalten, dass diese durch eine normale Firewall auf Netzwerkebene oder auf Layer 7[9] NICHT verhindert werden können. Genauso sind die Sicherheitsempfehlungen für die Programmierung der Web Application zwar essenziell, aber um eine umfassende Sicherheit zu erlangen, ist eine Web Application Firewall unumgänglich. Diese schützt den Webserver und letztendlich die Anwendungen und Daten im Backend vor bösartigen Cyberangriffen.

WAS IST EINE WEB APPLICATION FIREWALL?

Eine Web Application Firewall (kurz WAF) schützt die eingesetzte Anwendung auf dem Webserver und schützt Layer 7: Im OSI-Schichtenmodell ist das die Application-Ebene und stellt die Schnittstelle dar, bei der die Nutzer mit den Anwendungen auf dem Webserver kommunizieren. Beispiele dafür sind Client-Server-Prozesse wie das Aufrufen von Webdiensten via Browser. Eine WAF analysiert den Datenaustausch zwischen Clients und Webservern und prüft alle eingehenden Anfragen und Antworten an und vom Webserver. Wenn bestimmte Inhalte als verdächtig eingestuft werden, wird der Zugriff mit der WAF verhindert, ein Angriff auf sensible Daten wird abgewehrt. Eine WAF in Kombination mit einer Netzwerk-Firewall steigert das Sicherheitsniveau deutlich und ist im Zuge der steigenden Nutzung von Webanwendungen unverzichtbar.

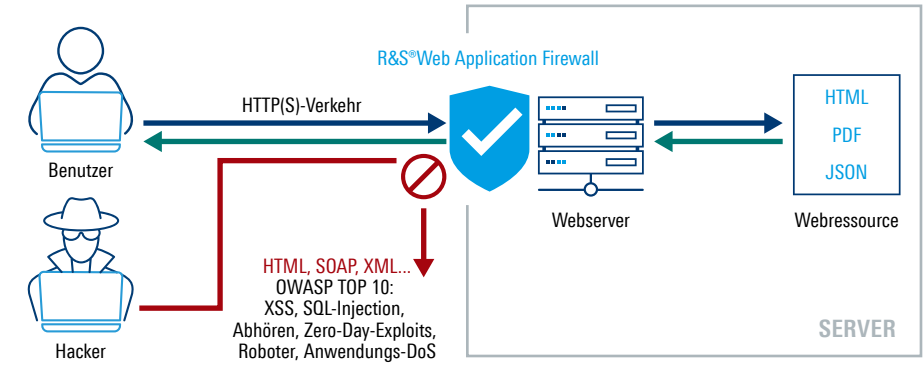

Abbildung 3: Effektive Sicherheit gegen eine Vielzahl von Angriffen

[9] Layer 7: Im OSI-Schichtenmodell ist es die Application-Ebene und stellt die Schnittstelle dar, bei der Nutzer mit den Anwendungen auf dem Webserver kommunizieren. Beispiele dafür sind z. B. E-Mail oder Client-Server-Prozesse wie das Aufrufen von Webdiensten via Browser.

5.1 R&S®Web Application Firewall von Rohde&Schwarz Cybersecurity

Um das Onlinezugangsgesetz sicher auf den Weg zu bringen, ist der Rat von Experten gefragt: Dazu gehört Rohde&Schwarz Cybersecurity. Wir haben seit über 20 Jahren Erfahrung auf dem Gebiet „Web Application Security“. Die R&S®Web Application Firewall ist bei zahlreichen Akteuren aus der Wirtschaft und bei staatlichen Behörden im Einsatz und ist durch die französische Cybersicherheitsbehörde ANSSI zertifiziert.

DIE VORTEILE AUF EINEN BLICK:

- Schützt öffentlich zugängliche und interne Webanwendungen und APIs vor TOP-10-OWASP-Angriffen (Webanwendungen und APIs)
- Effektive Sicherheit gegen eine Vielzahl von Angriffen durch Analyse des Benutzerverhaltens, künstliche Intelligenz, IP-Reputationsanalyse einschließlich automatisierter Angriffe (Bots)
- Geringere Gesamtbetriebskosten dank eines einzigartigen Workflow-Management-Systems zur Definition einfach zu implementierender und flexibler Sicherheitsrichtlinien
- Lokale und hybride/ Multi-Cloud-Bereitstellung
- Verschiedene Einsatzoptionen sind verfügbar: On-Premises, Public Cloud oder SaaS[10]
- Eine in Europa zertifizierte Lösung

[10] Beim Software-as-a-Service Modell wird alles von Rohde&Schwarz Cybersecurity verwaltet.

So geht die R&S®Web Application Firewall mit den 10 wichtigsten OWASP-API-Bedrohungen um:

OWASP-Bedrohung (API)	Steuerung durch R&S®Web Application Firewall
A1 – BROKEN OBJECT LEVEL AUTHORIZATION (BOLA)	▼
A2 – BROKEN AUTHENTICATION	▼
A3 – EXCESSIVE DATA EXPOSURE	✕
A4 – LACK OF RESOURCES & RATE LIMITING	✕
A5 – BROKEN FUNCTION LEVEL AUTHORIZATION	▼
A6 – MASS ASSIGNMENT	✕
A7 – SECURITY MISCONFIGURATION	▼
A8 – INJECTIONS	✕
A9 – IMPROPER ASSETS MANAGEMENT	✕
A10 – INSUFFICIENT LOGGING & MONITORING	▼

▼ Reduzierung ✕ Beseitigung

WEITERE INFORMATIONEN

Weiteres Material wie Whitepaper, Webinare und Produkt-Flyer zur R&S®Web Application Firewall finden Sie auf unserer Webseite:

www.rohde-schwarz.com/cybersecurity/ozg

Rohde & Schwarz Cybersecurity
Das IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity schützt digitale Informationen und Geschäftsprozesse von Unternehmen und öffentlichen Institutionen weltweit vor Cyberangriffen. Der IT-Sicherheitsexperte bietet innovative Datensicherheitslösungen für Cloud-Umgebungen, erweiterte Sicherheit für Websites, Webanwendungen und Webservices sowie Netzwerkverschlüsselung, Desktop- und Mobile-Security. Die vertrauenswürdigen Sicherheitslösungen werden nach dem Security-by-Design-Ansatz entwickelt und verhindern Cyberangriffe proaktiv.

Rohde & Schwarz
Rohde & Schwarz ist ein führender Lösungsanbieter in den Geschäftsfeldern Messtechnik, Broadcast- und Medientechnik, Aerospace | Verteidigung | Sicherheit sowie Netzwerke und Cybersicherheit. Mit seinen innovativen Produkten der Kommunikations-, Informations- und Sicherheitstechnik unterstützt der Technologiekonzern professionelle Anwender aus Wirtschaft und hoheitlichem Sektor beim Aufbau einer sicheren und vernetzten Welt. Der Firmensitz ist München. Das internationale Geschäft wird in mehr als 70 Ländern über Tochterfirmen betrieben. In Asien und Amerika steuern regionale Hubs die Geschäfte.

Partner:
THE BRISTOL GROUP Deutschland GmbH
Robert-Bosch-Str. 13 | 63225 Langen
Telefon: +49 (0) 6103 20 55 314
E-Mail: info@bristol.de
www.bristol.de

Rohde & Schwarz Cybersecurity GmbH
www.rohde-schwarz.com/cybersecurity

Version 01.00 | Mai 2020 (sch)
Onlinezugangsgesetz & Datenschutz: Mit Sicherheit zur digitalen Behörde
Titelbild: ©www.istock.com - piranka