Bitdefender

WHITEPAPER

Extrem zunehmende IT-Kriminalität erfordert spezialisierte Dienstleister

Extrem zunehmende IT-Kriminalität erfordert spezialisierte Dienstleister

Weltweit agierende Hackergruppen entwickeln ihre Angriffsmethoden ständig weiter. Den Schutz von Daten und Systemen können herkömmliche IT-Abteilungen schon lange nicht mehr garantieren.

Hektisches Treiben im Bundeskriminalamt, dann verlässt am 30. Mai 2024 eine Pressemitteilung die Büroräume: „Die Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) – und das Bundeskriminalamt (BKA) haben am 28. und 29.05.2024 in einer international abgestimmten Aktion gemeinsam mit Strafverfolgungsbehörden aus den Niederlanden, Frankreich, Dänemark, Großbritannien, Österreich sowie den USA, unterstützt durch Europol und Eurojust, mehrere der derzeit einflussreichsten Schadsoftware-Familien vom Netz genommen."

Der Erfolg kann sich sehen lassen: Weltweit wurden im Zuge der Operation Endgame über hundert Server beschlagnahmt und mehr als 1.300 kriminell genutzte Domains unschädlich gemacht. Die Aktion richtete sich gegen die Gruppierungen hinter den Schadsoftware-Familien IcedID, SystemBC, Bumblebee, Smokeloader, Pikabot und Trickbot, die als sogenannte Dropper für die Erstinfektion von Computersystemen dienen. Anschließend laden sie weitere Schadsoftware wie etwa Ransomware nach.

Um das Vorgehen der Täter zu analysieren, ihre Standorte zu identifizieren und weitere Informationen zu sammeln, die zu einer Ergreifung führen können, arbeiten die Behörden mittlerweile häufig mit Partnern aus der Security-Industrie zusammen. Im Fall der Operation Endgame waren zum Beispiel die Firmen Bitdefender, Cryptolaemus, Sekoia, Shadowserver, Team Cymru, Prodaft, Proofpoint, NFIR, Computest, Northwave, Fox-IT, Have I Been Pwned?, Spamhaus und DIVD an den Ermittlungen beteiligt.

Insbesondere Bitdefender engagiert sich bereits seit Jahren in der internationalen Bekämpfung von Cyberkriminalität. So trug das Unternehmen beispielsweise 2023 mit seinem Know-how dazu bei, dass der finnische Drogenmarktplatz Piilopuoti im

Dark Web geschlossen werden konnte. Im gleichen Jahr unterstützte Bitdefender das FBI beim Zerschlagen eines Botnets aus IoT-Proxys, die Hacker für kriminelle Aktivitäten verwendeten. Zwei Jahre zuvor hatte die Firma den technischen Background für die Analyse der Ransomware Sodinokibi/REvil geliefert und betroffenen Personen und Institutionen über die Website No More Ransom ein kostenloses Entschlüsselungs-Tool zur Verfügung gestellt. Zusammen mit einer Reihe weiterer Firmen zählte Bitdefender kurz nach der Gründung des Portals im Jahr 2016 zu den ersten Partnern des Projekts.

Ständig aktualisiertes technisches Fachwissen nötig

Dass Behörden im Bereich der Cybersicherheit immer wieder mit Bitdefender zusammenarbeiten, kommt nicht von ungefähr. Das Unternehmen gilt bereits seit vielen Jahren als Marktführer bei den Security-Anbietern und hat sich mit seinen Produkten und Dienstleistungen für Unternehmen einen ausgezeichneten Ruf erarbeitet. Das stetig aktualisierte Fachwissen der Hersteller von Sicherheitsprodukten macht sie für Strafverfolgungsbehörden besonders wichtig. Die Unternehmen beschäftigen sich tagtäglich mit neu entdeckten Sicherheitslücken und den Tricks krimineller

Hacker. Ihre Computersysteme suchen in den Internet-Datenströmen kontinuierlich nach neuer und bekannter Malware sowie Angriffstechniken, wobei sie die Häufigkeit zählen und neue Virenvarianten registrieren. Sie können den Behörden damit Echtzeitinformationen zur Verbreitung bestimmter Bedrohungsaktivitäten liefern. Außerdem zeigen sie mithilfe von Statistiken und Diagrammen, von welchen Gruppen und Ländern die Angriffe ausgehen und welche Ziele diese bevorzugen.

Durch die stets aktuellen Daten lassen sich auch Trends erkennen. Für die Strafverfolgungsbehörden, die häufig international kooperieren, bilden diese Daten ein wertvolles Grundgerüst für ihre Arbeit. Die Erkenntnisse aus diesen Informationen fließen zudem in die Produkt- und Service-Entwicklung der Hersteller ein. Das wiederum schafft die Voraussetzung dafür, dass aktive Angriffe auf die Infrastruktur von Firmen und Endanwendern frühzeitig erkannt werden können.

Gleichzeitig verfolgen die Security-Unternehmen die Berichterstattung in den internationalen Medien über kürzlich bekannt gewordene Attacken auf Unternehmen, Krankenhäuser, Regierungseinrichtungen und öffentliche Infrastruktur wie etwa Kraftwerke oder Staudämme. Ihre Analytiker sammeln alle verfügbaren Informationen über diese Angriffe und versuchen, das Vorgehen und die Taktik der Kriminellen nachzuvollziehen. Auf diese Weise stoßen sie oft auf bisher unbekannte Sicherheitslücken und Fehlkonfigurationen. Häufig ermöglichen aber auch risikoreiche Prozesse innerhalb eines Betriebs erst Ransomware-Angriffe oder den Diebstahl vertraulicher Informationen.

Dieses Know-how verwenden die Security-Firmen für die Beratungsleistungen, die sie ihren Kunden oder den Behörden anbieten. Für die erforderlichen, oft umfangreichen Analysen benötigen sie jedoch genügend Ressourcen. Bei Bitdefender beispielsweise besteht die rund 1.800 Mitarbeiter umfassende Belegschaft zu mehr als der Hälfte aus Sicherheitsforschern und Technikern. Nur mit der geballten Praxiserfahrung dieser Angestellten ist es möglich, zur Strafverfolgung weltweit agierender, krimineller Gruppen aktiv beitragen zu können.

Denn die Bekämpfung von Cyberkriminalität ist heute eine internationale Aufgabe. Die Akteure arbeiten über Ländergrenzen hinweg in weltweit agierenden Netzwerken zusammen. Das erfordert das Know-how international tätiger Security-Firmen, die aktuelle Bedrohungen richtig einschätzen und für das jeweilige Unternehmen angepasste Sicherheitsstrategien entwickeln. Die kriminellen Gruppen entwickeln immer neue Methoden und Tools, mit denen sie die Sicherheitssysteme von Unternehmen, Behörden und Organisationen attackieren. Dank ihres umfassenden Wissens über aktuelle Hacker-Techniken und jahrzehntelanger Erfahrung können Sicherheitsfirmen wie Bitdefender Cyberkriminalität wirksam bekämpfen.

Sicherheitsrisiken erkennen und managen

Um Schwachstellen im Security-Konzept zu finden oder auch die Wirksamkeit des gesamten Konzepts einem Stresstest zu unterziehen, greifen Unternehmen auf professionelle IT-Security-Firmen und Verfahren des Angriffsflächen-Managements zurück (Attack Surface Management, ASM). Beim sogenannten Red Teaming werden einzelne Mitarbeiter oder auch ganze Gruppen mit entsprechender Erfahrung vom Unternehmen dazu autorisiert, die Position eines Angreifers einzunehmen, der versucht, in die Systeme einzudringen. Häufig führen solche Tests auch „ethische Hacker“ durch, die die Angriffsmethoden krimineller Gruppen kennen und deren Verhaltensweisen nachahmen können.

Das Angriffsflächen-Management darf nicht verwechselt werden mit einem Penetrationstest (Pentest). Dabei handelt es sich um einen einmaligen Belastungstest für die Security und die Datensicherheit eines Unternehmens, der zum Ziel hat, bislang unentdeckte Schwachstellen zu identifizieren. Ein Angriffsflächen-Management ist hingegen ein kontinuierlicher Prozess, der so weit wie möglich automatisch abläuft. Das erfordert eine langfristige Perspektive, da die Hacker ihre Angriffsmethoden ständig weiterentwickeln und gleichzeitig neue Software und Updates auch neue Schwachstellen mit sich bringen. Über eine Inventarisierung und Analyse aller mit dem Internet verbundenen Assets eines Unternehmens und durch eine kontinuierli-

che Überwachung des Netzwerks bauen Security-Spezialisten wie Bitdefender einen übergreifenden Schutzschirm für das Unternehmen auf. Dieser Schutzschirm wird anschließend ständig aktualisiert und um neue Informationen und Analysen ergänzt.

Eng verbunden mit dem Angriffsflächen- ist ein Risiko-Management. Dieses Konzept basiert auf der Erkenntnis, dass sich die Risiken für den Schutz, die Integrität und die Verfügbarkeit der Daten eines Unternehmens aufgrund der schnellen Entwicklungszyklen in der IT niemals komplett eliminieren lassen. Es geht also darum, die Risiken zu beherrschen, sie so weit wie möglich zu reduzieren und für das Unternehmen ein vertretbares Risikoniveau zu erreichen. Auch eine Bewertung der Assets eines Unternehmens zählt zum Pflichtprogramm: Welche Daten oder Dienstleistungen sind überlebenswichtig? Betreibt eine Firma beispielsweise einen Onlineshop, so könnte ein Ausfall über mehrere Tage oder Wochen hinweg den Ruin bedeuten. In anderen Fällen sind es Steuerungssysteme für Maschinen oder Daten aus der technischen Entwicklung, die auf keinen Fall den Dienst versagen beziehungsweise in fremde Hände gelangen dürfen. Diese Assets zu benennen und die Sicherheitsrisiken zu analysieren, denen sie ausgesetzt sind, ist die wichtigste Aufgabe des Risiko-Managements.

Für die Bewertung der Sicherheitsrisiken von Assets und neu entdeckten Schwachstellen sind erfahrene Sicherheitsexperten erforderlich. Sie sehen, wo sich Konstellationen ergeben könnten, die Angriffe durch Kriminelle ermöglichen oder zumindest erleichtern. Sie wissen auch, wie und wo ein Hacker bei einer Software nach Schwachstellen sucht, die ihm den Zugang zu weiteren Systemen oder sogar zum Netzwerk öffnen. Security-Hersteller wie Bitdefender ermöglichen es Unternehmen, ihr über Jahrzehnte gesammeltes Know-how zu nutzen und beim Aufbau eines eigenen Angriffsflächen- und Risiko-Managements einzusetzen.

Ransomware-Angriff auf IT-Dienstleister

Jedes Jahr im Herbst veröffentlicht das BSI (Bundesamt für Sicherheit in der Informationstechnik) seinen Bericht zur Lage der IT-Sicherheit in Deutschland. Die aktuelle Ausgabe stammt zwar bereits vom November 2023, die dargestellten Trends werden jedoch durch Daten aus anderen Quellen auch für das Jahr 2024 bestätigt. So hatte es einer der größten Sicherheitsvorfälle der letzten Jahre nicht mehr in den Bericht geschafft. Ende Oktober 2023 ereignete sich ein Ransomware-Angriff auf die Firma Südwestfalen-IT (SIT), einen Dienstleister, der vor allem Kommunen zu seinen Kunden zählt. Bei solchen Ransomware-Attacken dringen die Kriminellen ins Netzwerk einer Firma ein, infizieren die Systeme und verschlüsseln zu einem bestimmten Zeitpunkt die Datenträger. Erst nach der Bezahlung eines Lösegelds erhalten die Opfer einen Entschlüsselungscode.

Ab dem 30. Oktober wurden die Auswirkungen des Ransomware-Angriffs für die Kunden von Südwestfalen-IT, also für die Gemeinden und ihre Bürger, spürbar: Melde-, Pass- und Zulassungsstellen mussten ihre Arbeit einstellen, die Sozialkassen konnten keine Auszahlungen mehr vornehmen. Etwa 70 Kommunen mussten alle mit der IT in Verbindung stehenden Vorgänge aussetzen, in weiteren rund 130 Gemeinden gab es Teilausfälle. Teilweise funktionierte eine Website nicht mehr, in einem anderen Fall musste beispielsweise das Standesamt seine Pforten schließen. Experten gehen davon aus, dass die Kommunen auf den entstandenen Kosten sitzen bleiben. Bei den Cybersicherheitsvorfällen in deutschen Unternehmen verzeichnen BSI, Bundeskriminalamt (BKA) und das Bundesinnenministerium einen bereits seit mehreren Jahren anhaltenden Trend: Straftaten im IT-Bereich werden zunehmend von Tätern im Ausland begangen. Im Jahr 2023 nahm die Zahl dieser Auslandstaten um 28 Prozent zu. Die Inlandstaten stagnierten in diesem Zeitraum auf hohem Niveau.

Als weiterer Trend kristallisiert sich die weiter zunehmende Professionalisierung und Arbeitsteilung bei den Kriminellen heraus. Sie greifen immer mehr auf Dienstleistungen wie „Crime-as-a-Service“ zurück, die sie von anonym und dezentral arbeitenden Tätergruppen beziehen, die ihrerseits eine Gewinnbeteiligung erhalten. Auf diese Weise können auch Gruppen ohne größeres Fachwissen im Bereich der Cyberkriminalität aktiv werden.

Ransomware bleibt größte Gefahr für Unternehmen

Ransomware stellt nach wie vor die größte Bedrohung für Unternehmen, staatliche Stellen und Organisationen dar. Laut den offiziellen Zahlen gingen 2023 bei der Polizei über 800 Anzeigen wegen Erpressungsversuchen in Zusammenhang mit Datenverschlüsselung ein. Die Dunkelziffer dürfte jedoch viel höher liegen. Der Branchenverband Bitkom schätzt den entstandenen gesamtwirtschaftlichen Schaden durch direkte Cyberangriffe auf rund 148 Milliarden Euro im Jahr 2023. Betrachtet man die weltweite Entwicklung, zeichnet sich ab, dass sich die Cyberkriminellen zunehmend auf kleine und mittlere Firmen konzentrieren. Diese können zwar keine so hohen Lösegeldsummen bezahlen wie Großunternehmen, verfügen andererseits aber in vielen Fällen auch nicht über die personellen und finanziellen Ressourcen, um ein ähnlich umfassendes Security-Konzept umzusetzen.

Ein aktueller Trend bei Ransomware-Angriffen ist die mehrstufige Erpressung. Um ihren Geldforderungen mehr Nachdruck zu verleihen, verschlüsseln die Kriminellen die Daten auf den Systemen ihrer Opfer nicht nur. Zusätzlich stehlen sie die Daten, indem sie sie vor der Verschlüsselung auf ihre eigenen Server kopieren, und drohen damit, die Datensätze im Dark Web zu veröffentlichen. Das kann vertrauliche Firmenunterlagen zu laufenden Produktentwicklungen genauso betreffen wie Details aus Verträgen mit Zulieferern und Kunden.

Teilweise kommt noch eine dritte Eskalationsstufe hinzu, nämlich die Drohung mit Distributed-Denial-of-Service-Angriffen (DDoS) auf die Web-Infrastruktur des Unternehmens. Ein solcher Angriff führt in der Regel dazu, dass die Website und Shopsysteme nicht mehr funktionieren, wodurch die Firma einen herben Imageschaden erleidet. Mit dem Hinweis auf die Folgen eines DDoS-Angriffs versuchen die Kriminellen, den Druck auf ihre Opfer noch weiter zu erhöhen.

Darüber hinaus nutzen auch so genannte Hacktivisten DDoS-Angriffe, um beispielsweise Propaganda zu verbreiten. Sie richten ihre Attacken vorzugsweise gegen Behörden, öffentliche Einrichtungen, das Finanzwesen und Verkehrsbetriebe. Das Bundeskriminalamt (BKA) zitiert in diesem Zusammenhang Daten der Deutschen Telekom, wonach es durchschnittlich zu 1.875 DDoS-Attacken pro Monat kommt. Die Angriffe erfolgen mit einer durchschnittlichen Bandbreite von 658 Mbit/s und dauern im Schnitt etwa 45 Minuten.

Die Tricks der Kriminellen

Um in die Rechnernetze von Firmen einzudringen, verwenden die Banditen in erster Linie Phishing-Nachrichten. Besonders gefährlich ist in diesem Zusammenhang das Spear-Phishing, bei dem sich die Täter beispielsweise als IT-Administrator ausgeben und eine bestimmte Person innerhalb der Firma zur Eingabe ihrer Log-in-Daten auf einer gefälschten Website auffordern. Diese Daten fangen sie dann ab.

Eine andere Masche nennt sich Whaling. Dabei schicken die Kriminellen eine E-Mail an eine Führungskraft im Unternehmen, in der sie sich als Kunde oder Handelspartner ausgeben. Sie schreiben, dass sich ihre Kontoverbindung geändert habe, und bitten um die Überweisung des anstehenden Rechnungsbetrags auf das neue Konto, das natürlich ihnen gehört. Trifft das Geld ein, heben die Betrüger es sofort ab und verschwinden.

Beide Betrugsmaschen erfordern ein professionelles Vorgehen der Gangster. Sie müssen im Vorfeld Namen, Funktionen und E-Mail-Adressen der Zielpersonen sowie die Geschäftspartner des Unternehmens recherchieren und einen Webauftritt beziehungsweise das Design einer geschäftlichen E-Mail fälschen. Das BSI beobachtet, dass bei der Formulierung der Texte der Phishing-Nachrichten zunehmend KI-Systeme wie ChatGPT zum Einsatz kommen. Auf diese Weise konnten die Kriminellen in den vergangenen Monaten Rechtschreib- und Grammatikfehler minimieren sowie die Nutzung ungewöhnlicher Begriffe vermeiden. Phishing-Mails sind heutzutage deshalb deutlich schwieriger zu erkennen als früher.

Viele Firmen wollen sich gegen Angriffe schützen, indem sie eine Cyberversicherung abschließen. Doch nachdem anfangs zahlreiche Versicherungsunternehmen

entsprechende Verträge entwickelten, haben sich mittlerweile viele wieder aus diesem Markt zurückgezogen, da die Schadenaufwendungen plus Betriebskosten die Prämieneinnahmen überstiegen. Aus Sicht der von den Versicherungskonzernen anvisierten Kunden ist es ohnehin keine gute Idee, sich auf seine Cyberversicherung zu verlassen und dafür eventuell den Schutz gegen die ständig wachsende Bedrohung durch kriminelle Cyberbanden zu vernachlässigen. Mehr Erfolg verspricht die ständige Weiterentwicklung der eigenen Schutzmaßnahmen, auch die Anpassung an sich permanent verändernde Angriffstechniken gilt als wichtiger Baustein. Das kann entweder intern durch eine dedizierte Security-Abteilung erfolgen oder durch den Rückgriff auf die Angebote von Unternehmen, die sich auf Cybersicherheit spezialisiert haben.

Kooperationen mit Sicherheitsanbietern

Die wirtschaftlichen Risiken durch Cyberangriffe nehmen immer weiter zu, viele Organisationen leiden unter Ransomware-Angriffen. Sie müssen deshalb erweiterte Sicherheitsvorkehrungen treffen, um nicht durch die Verschlüsselung oder den Diebstahl ihrer Daten hohe finanzielle Verluste und Imageschäden zu erleiden. Dazu fehlen den Unternehmen jedoch oft die finanziellen Ressourcen und die entsprechenden Fachkräfte.

Die Lösung liegt in diesen Fällen in der Kooperation mit erfahrenen Sicherheitsspezialisten. Diese Firmen können zum einen jederzeit auf aktuelle Daten der

Bedrohungslage zurückgreifen, andererseits verfügen sie auch über das notwendige Wissen und die modernsten Tools zur Umsetzung einer wirksamen und auf die spezielle Konstellation bei einem Unternehmen zugeschnittenen Sicherheitsstrategie. Aufgrund des hohen Datenschutzniveaus in der Europäischen Union empfehlen sich vor allem europäische Unternehmen wie die in Rumänien beheimatete Firma Bitdefender als Partner.

US-amerikanische Unternehmen unterliegen hingegen den Regeln des 2001 verabschiedeten USA Patriot ACT. Er ermöglicht es US-Behörden wie FBI, CIA oder NSA in manchen Fällen, ohne richterliche Kontrolle auf Server von US-Unternehmen zuzugreifen. Das gilt auch für die Server von Tochterunternehmen im Ausland, und zwar selbst dann, wenn regionale Gesetze einen Zugriff verbieten. Im Visier der Geheimdienste sind dabei nicht nur die Daten von Terrorverdächtigen, sondern auch Geschäftsgeheimnisse von Firmen außerhalb der USA. Experten vermuten sogar, dass die NSA regelmäßig alle Daten abgreift, die auf Servern amerikanischer Unternehmen liegen.

Cybersicherheit ist gesellschaftsrelevant

Angesichts der immer weiter zunehmenden Bedrohung der Industrie durch Cyberangriffe und finanziellen Folgeschäden ist es nicht übertrieben, bei Security-Unternehmen wie Bitdefender einen gesellschaftlichen Auftrag zu sehen. Die Angriffe gehen in zunehmendem Maße von kriminellen Gruppen im Ausland aus, die von ihren Regierungen nichts zu befürchten haben. Offensichtlich greifen die dortigen Strafverfolgungsbehörden nur dann ein, wenn die Betrüger heimische Unternehmen angreifen. Bei Attacken gegen ausländische Firmen sehen sie hingegen weg.

Mehr noch: Immer wieder werden besonders raffinierte Angriffe bekannt, die von Hackergruppen ausgehen, die mit ausländischen Geheimdiensten in Verbindung stehen.

Die Security-Firmen erfüllen ihren gesellschaftlichen Auftrag, indem sie Unternehmen, staatlichen Institutionen und Organisationen jeder Größenklasse Beratung und Schutz vor Cyberattacken anbieten. Das umfasst die Analyse der vorhandenen Sicherheitseinrichtungen des Unternehmens, das Aufzeigen von Schwachstellen und die gemeinsam mit dem Kunden vorgenommene Suche nach einer passenden technischen Lösung genauso wie das Angebot einer längerfristigen Zusammenarbeit. Bitdefender unterstützt Unternehmen in diesem Zusammenhang mit den Diensten seines Security Operation Centers (SOC) in Form sogenannter Managed-Detection-and-Response-Services (kurz: MDR-Services).

Ein SOC besteht aus einem Team von Sicherheitsexperten, die rund um die Uhr die IT-Infrastruktur eines Unternehmens überwachen und Anomalien frühzeitig erkennen. Dadurch schaffen sie es, schnell Gegenmaßnahmen zu ergreifen. Es ist wichtig, dass nicht nur ein hoher Erkennungsgrad mit kurzen Antwortzeiten gewährleistet wird, sondern auch das präzise Herausfiltern relevanter Alarme, um den Arbeitsaufwand für den Auftragnehmer zu minimieren.

Die gemeinnützige amerikanische MITRE Corporation testet jedes Jahr nach einem immer wieder überarbeiteten Verfahren die MDR-Services verschiedener Security-Anbieter. Mittlerweile liegen die Ergebnisse des Tests aus dem laufenden Jahr 2024 vor: Er bescheinigt Bitdefender eine hervorragende Bedrohungserkennung, gut umsetzbare Erkenntnisse und lobt das Engagement der Firma für die Verringerung von Fehlalarmen. Ein Blog-Beitrag fasst das Ergebnis der Untersuchung zusammen (https://tinyurl.com/yc3d9uvb).

Ein externes SOC wie das von Bitdefender lässt sich von den Kunden einfach in die eigenen Abläufe einbinden und kostet zudem erheblich weniger als der Aufbau einer eigenen Abteilung. Dank seiner Erfahrung und des Fachwissens der Mitarbeiter eignet sich Bitdefender dabei als idealer Partner.

Über Bitdefender

Bitdefender ist ein weltweit führender Anbieter von Cybersicherheitslösungen zur Abwehr, Erkennung und Reaktion auf Bedrohungen. Bitdefender schützt mehrere Millionen von Endverbrauchern sowie IT-Umgebungen in Unternehmen und im öffentlichen Sektor. Die Lösungen sind in hohem Maße anerkannt als Mittel, Bedrohungen zu beseitigen, die Privatsphäre, digitale Identitäten und Informationen zu schützen sowie die Resilienz der IT gegenüber Cyberbedrohungen zu stärken. Dank umfangreicher Investitionen in Forschung und Entwicklung entdecken die Bitdefender Labs minütlich Hunderte neuer Bedrohungen und validieren täglich Milliarden von Bedrohungsanfragen. Das Unternehmen hat in seiner Geschichte bedeutende Innovationen in den Bereichen Anti-Malware, IoT-Sicherheit, Verhaltensanalyse und künstliche Intelligenz entwickelt. Seine Technologie wird von mehr als 180 der weltweit bekanntesten Technologiemarken lizenziert. Bitdefender wurde 2001 gegründet und hat Kunden in über 170 Ländern mit Niederlassungen auf der ganzen Welt. Weitere Informationen finden Sie unter www.bitdefender.de.

Trusted. Always.

Kontaktieren Sie uns:

sales-dach@bitdefender.com