MYRA

WARUM ES SICH RECHNET:

Der ROI von Application Security im E-Commerce

Warum es sich rechnet: Der ROI von Application Security im E-Commerce

Executive Summary

Eine funktionierende Internet-Infrastruktur ist für einen Online-Händler absolut geschäftskritisch – das macht diese Branche für Cyberkriminelle außerordentlich attraktiv. Sie nutzen diesen Umstand aus und richten ihren Fokus zunehmend auf diesen Wirtschaftszweig. 85 % der Händler erklärten in einer Studie der Bug-Bounty-Plattform Yeswehack, dass sie von IT-Sicherheitsvorfällen betroffen waren.[1] Mit knapp 68 % verzeichnete die Mehrheit der Händler zwischen einer und 20 Cyberattacken in den letzten zwölf Monaten.

Teil der Lösung dieses Problems sind Investitionen in Application Security wie sie Myra Security anbietet. Sie schützt ganzheitlich vor Cyberangriffen, während sie zeitgleich die Performance der geschützten Infrastruktur verbessert. Beides sind wesentliche Bestandteile für den Unternehmenserfolg von E-Commerce-Unternehmen.

IT-Sicherheit als sinnvolles Invest für E-Commerce-Treibende

Die Bestimmung des Returns on Investment (ROI) für Security-Investitionen kann sehr aufwendig sein. Niemand wird angesichts der aktuellen Cyber-Bedrohungslage bestreiten, dass ein Sicherheitsbudget notwendig ist. Das Problem liegt vielmehr darin, den Mehrwert von getätigten oder anstehenden Anschaffungen neuer Hard- oder Software zu belegen: Security-Einkäufe zeichnen sich dadurch aus, dass sie Schäden vermeiden. Wie aber beziffert man einen Schaden, der nicht eingetreten ist? Mit der folgenden Formel zeigen wir einen Weg, wie sich der Mehrwert einer Schutzlösung wie der Application Security von Myra für den Unternehmenserfolg ermitteln lässt. Die Beispielfaktoren für die einzelnen Parameter der Formel werden auf den folgenden Seiten näher erläutert.

$$ROI = \frac{\Delta\ Revenue + \Delta\ Cost + \Delta\ Capex}{Invest}$$

1 www.t3n.de/news/cyberangriffe-handel-zunehmen-komplex-1489019

Revenue

Schauen wir uns den ersten Parameter der Gleichung an: Der Impact einer Application-Security-Lösung auf den Umsatz Ihres Unternehmens resultiert aus unterschiedlichen Effekten, die sich mittels belastbarer Zahlen sowie Bewertungen unterschiedlicher Risiken ermitteln lassen.

Faktor 1: Downtime-Vermeidung

Stellen Sie sich vor, es ist Black Friday und Ihr Online-Shop ist nicht erreichbar. Die Ursache dafür ist in vielen Fällen ein DDoS-Angriff. Handelt es sich dabei um eine Ransom-Distributed-Denial-of-Service-Attacke (RDDoS), kommt zum Ausfall der Seite noch eine Erpressung mit Lösegeldforderung hinzu.

Eine solche ungeplante Downtime – egal, durch welche Angriffsart sie schlussendlich herbeigeführt wird – kann für den Shop-Betreiber schwerwiegende finanzielle Konsequenzen haben. Die Verluste lassen sich beispielsweise mit einem der mittlerweile zahlreich im Internet verfügbaren Online-Rechner minutengenau kalkulieren, zum Beispiel mit www.gremlin.com/ecommerce-cost-of-downtime

Darüber hinaus ergeben sich weitere Folgekosten und Ineffizienzen, wie etwa Marketing-Ausgaben, die ins Leere laufen sowie Neukunden und Customer Lifetime Values, die verloren gehen und im schlimmsten Fall zum Wettbewerb abwandern. Zur holistischen Bestimmung des monetären Wertes einer Downtime-Vermeidung stellt Myra Ihnen auf Nachfrage gerne eine separate Anleitung zur Verfügung.

Faktor 2: Performance

Neben der zuverlässigen Erreichbarkeit spielen auch die Seitenladezeiten Ihres Online-Shops eine bedeutende Rolle. Die Schnelligkeit, mit der Inhalte ausgeliefert werden, hat einen entscheidenden Einfluss auf den Umsatz. Lange Ladezeiten wirken sich nachweislich negativ auf die Conversion Rate und den Traffic einer Website aus. Hier gibt es häufig noch Optimierungspotenzial.

2a: Conversion Rate

Laut einer Untersuchung von Akuma erwarten 83 % der Besucher:innen, dass eine Webseite in unter drei Sekunden lädt. Pro Sekunde Ladezeit fällt die Conversion Rate demnach um 7 % ab. Um ergänzend das Beispiel Amazon zu bemühen: Der E-Commerce-Riese spricht davon, dass eine um 100ms schlechtere Ladezeit einen Umsatzrückgang von 1 % bedeutet.[2]

2b: Traffic

Die Ladezeit einer Website hat darüber hinaus auch Einfluss auf das Listing bei den Suchmaschinen und damit Ihren Traffic: Seit Juli 2018 ist beispielsweise die Ladezeit ganz offiziell ein Rankingfaktor für die mobile Suche bei Google. Für die Desktop-Suche gilt ein solcher Faktor bereits seit 2012.[3] Die Application Security von Myra komplettiert Schutzlösungen mit einem integrierten Content Delivery Network (CDN). Ein CDN sorgt für Schnelligkeit beim Seitenaufbau. Das Myra High Performance CDN liefert alle statischen und dynamischen Elemente Ihrer Website blitzschnell aus und sorgt damit nicht nur für ein überzeugendes User-Erlebnis, sondern unterstützt die Auffindbarkeit bei Suchmaschinen und in der Konsequenz die Traffic-Generierung sowie die Optimierung der Conversion Rate.

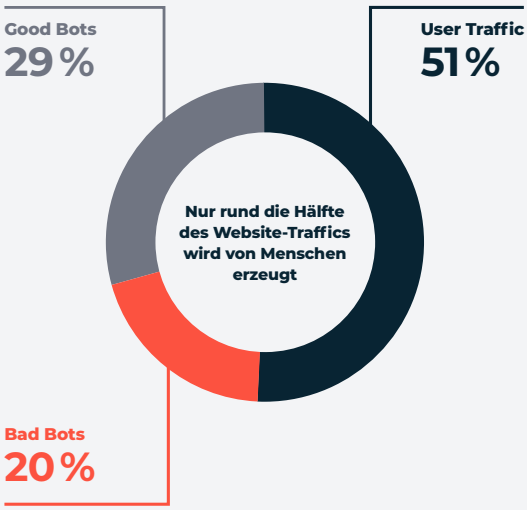
2 blog.mi.hdm-stuttgart.de/index.php/2022/01/17/drei-sekunden-sind-zu-lang-auswirkung-der-ladezeit-von-webseiten-auf-die-user-experience/

3 www.onlinemarketing.de/seo/google-update-mobile-page-speed-rankingfaktor

Faktor 3: Wettbewerbsnachteile durch schädliche Bots vermeiden

Etwa die Hälfte aller Website-Zugriffe entfällt heute auf autonom agierende Bots. Rund 20 % gelten als potenziell gefährlich und stellen damit ein nicht zu unterschätzendes Risiko dar. Die Angriffsmethoden bösartiger Bots sind dabei genauso vielfältig wie die Geschäftsmodelle im E-Commerce: Sie scannen Online-Shops nach ausnutzbaren Schwachstellen, lesen Preisinformationen aus (Price Grabbing), blockieren Warenkörbe (Card Abandonment) oder versuchen, Nutzerkonten zu kompromittieren (Credential Stuffing). Allein diese wenigen Beispiele zeigen, dass sich das monetäre Risiko nur schwer bestimmen lässt und je nach Angriffsart unterschiedlich ausfallen kann.

Durch Einsatz einer Bot-Management-Lösung unterbinden Sie Bot-basierte Angriffe und steigern Ihren Umsatz entsprechend. Das in die Myra Application Security integrierte Deep Bot Management verwirft oder blockiert schädliche und unerwünschte Anfragen direkt. Myra erstellt für jeden Bot einen eindeutigen Fingerprint und erkennt Bots anhand dessen sehr schnell wieder. So können Sie auf jede Anfrage optimal reagieren, automatisierte Zugriffe zielgenau steuern und die Performance Ihrer Website verbessern.



Zur holistischen Bestimmung des monetären Mehrwertes einer Web Application Firewall (WAF), deren Bestandteil das Bot Management ist, stellt Myra Ihnen auf Nachfrage gerne eine separate Anleitung zur Verfügung.

Faktor 4: Umsatzeinbußen durch Reputationsverlust vermeiden

Stellen Sie sich vor, die Schlagzeile „Cyberkriminelle erbeuten Zahlungsdaten von Kunden" handelt von Ihrem Online-Shop. Die Folgen einer solchen Headline oder genauer gesagt, die Auswirkungen von Cyberangriffen auf die Reputation eines E-Commerce-Unternehmens sind nicht zu unterschätzen. Laut einer Studie der Werbeagentur Serviceplan und der Markenberatung Biesalski & Company ist der gute Ruf eines Unternehmens für bis zu einem Viertel des Umsatzes verantwortlich.[4]

Insbesondere Datenpannen (Data Breaches), zum Beispiel infolge eines Bot-basierten Credential-Stuffing-Angriffs, können den Ruf eines Online-Shops nachhaltig schädigen: Bei dieser Attacke testen Bots in kürzester Zeit massenhaft Nutzer/Passwort-Kombinationen. Die Treffer zu aktiven Accounts werden anschließend verkauft oder für weitere Attacken genutzt. Geraten Login-Details oder hochsensible Informationen wie beispielsweise die Bank- und Kontodaten in die Hand von Cyberkriminellen, ist das Vertrauen in den betroffenen Händler nachhaltig erschüttert. Das Medienecho, das oftmals bei Datenpannen auf dem Fuße folgt, schreckt zudem potenzielle Neukunden ab und potenziert den Schaden um ein Vielfaches.

Der Reputationsverlust als solcher lässt sich also nicht so eindeutig wie beispielsweise die finanziellen Auswirkungen einer durch eine DDoS-Attacke herbeigeführten Downtime beziffern. Dennoch: Leidet die Reputation eines Shops, kann das zu nachhaltigem Kundenverlust und somit zu finanziellen Einbußen führen.

4 www.anwalt.org/reputationsschaden
5 IBM Cost of a Data Breach Report 2022

Costs

Widmen wir uns dem zweiten Parameter der Gleichung: Die Absicherung von Webanwendungen hat nicht nur wie geschildert einen positiven Einfluss auf den Umsatz eines E-Commerce-Anbieters, sondern hilft auch Kosten zu vermeiden. Im Groben lassen sich drei Arten von Kosten unterscheiden – die beiden ersteren sind in der Höhe abhängig von der individuellen Risikobewertung der IT-Verantwortlichen.

Faktor 1: Kosten infolge von DSGVO-Verstößen vermeiden

Gehen wir einmal davon aus, ein Kunde entdeckt einen Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) in Ihrem Online-Shop und meldet diesen der zuständigen Aufsichtsbehörde. Dies kann teure Folgen haben: Zu den Aufwänden in Rechtsabteilungen und Anwaltskosten kommen noch Aufwände in der Presseabteilung, Ressourcen für den Kundenservice und vieles mehr. In die Kostenkalkulation müssen ebenfalls Strafzahlungen einbezogen werden, die gemäß des in Art. 83 Abs. 5 DSGVO festgelegten Bußgeldkataloges drohen können. Auch der Verwaltungsaufwand, den ein Verstoß gegen die DSGVO nach sich zieht, wie etwa die Meldung beim Bundesamt für Sicherheit in der Informationstechnik (BSI), ist ein Kostenfaktor, der sich durch den Einsatz eines entsprechend zertifizierten Security-Dienstleisters vermeiden lässt. Mit all diesen Faktoren können die finanziellen Folgen eines DSGVO-Verstoßes grob kalkuliert werden. Aus der Multiplikation des Risikofaktors in Prozent und der Höhe der veranschlagten Aufwände lässt sich dieses Kostenrisiko gut abschätzen.

Die DSGVO erstreckt sich im Übrigen auch auf Dienstleister und Drittanbieter: Im Falle der Online-Händler kann das zum Beispiel die eingesetzten Shop-Systeme betreffen. So erklärte die rheinland-pfälzische Landesdatenschutzbehörde im Juni 2022 die Nutzung der von Shopify verwendeten US-amerikanischen CDNs Fastly und Cloudflare für rechtswidrig und drohte einem Shop-Betreiber aus diesem Grund mit einem Bußgeld. Dieser war schlussendlich gezwungen, auf ein anderes Shop-System umzusteigen, um weiteren Ärger mit der Aufsichtsbehörde zu vermeiden.

DSGVO-Geldbußen nach Art. 83: bis zu 20 Millionen Euro oder bis zu 4 % des Jahresumsatzes

Auch DDoS-Schutzlösungen müssen DSGVO-konform sein. Sie sichern digitale Shops konsequent gegen Überlastungsangriffe auf der Anwendungsebene (Layer 7) ab. Der Betrieb eines solchen Schutzsystems erfordert allerdings ein Aufbrechen des verschlüsselten Datenverkehrs. Aus diesem Grund muss die Rechtssicherheit des eingesetzten IT-Dienstleisters genau geprüft werden, um juristisch auf der sicheren Seite zu sein.

Myra erfüllt strengste Anforderungen an Sicherheit und Compliance, einschließlich der DSGVO-Konformität. Wir lassen uns regelmäßig auditieren und zertifizieren. Shop-Betreiber, die unsere Lösungen einsetzen, können sich darauf verlassen, dass wir jederzeit nach höchsten Qualitätsstandards arbeiten und sie vor unangenehmen, kostenintensiven „Überraschungen“ aus dieser Richtung zuverlässig schützen.

Faktor 2: Kosten infolge eines Data Breaches vermeiden

Die Schlagzeile, die wir Ihnen bei der Erläuterung der Umsatzeinbußen durch Reputationsverlust vorgestellt haben, hat noch eine weitere Dimension. Angenommen, in Ihrem Unternehmen gab es einen Datenschutzvorfall. Dieser zieht eine lange Kette an administrativen Aufgaben nach sich, die Kosten in unterschiedlichsten Abteilungen verursachen. Analog zu DSGVO-Verstößen, haben Sie es auch bei Data Breaches mit Presseanfragen, Klagen und Beschwerden von Kunden zu tun, die je nach Schwere des Vorfalls hohe Aufwände und in der Konsequenz Kosten verursachen. Das weiter oben ausgeführte Gedankenexperiment greift dementsprechend nicht nur bei DSGVO-Verstößen, sondern auch bei Datenschutzverletzungen.

Das BSI stuft Angriffe auf Kundendatenbanken von Online-Shops als ein ernstzunehmendes Thema ein. Im Rahmen einer Studie hat das BSI Software-Produkte für Online-Shops auf Schwachstellen untersucht und dabei insgesamt 78 Sicherheitslücken gefunden – teilweise hatten diese gravierenden Auswirkungen auf das Sicherheitsniveau von Kundendaten.[6] Die Beseitigung solcher Lücken und die Abwicklung der durch Attacken entstandenen Schäden gehen häufig mit einem hohen finanziellen Aufwand einher.

Angreifer nutzen gezielt Schwachstellen in Webanwendungen aus, um in anfällige Systeme einzudringen und Daten zu manipulieren, zu stehlen oder zu löschen. Die Myra Hyperscale Web Application Firewall (WAF) blockiert bösartige Zugriffe, noch bevor diese Ihre Server erreichen. Damit bildet sie einen vorgelagerten Schutzwall gegen verschiedenste Angriffstechniken (OWASP Top 10 und mehr) sowie gegen Zero-Day-Exploits wie Log4j/Log4Shell. Mit eigens entwickelten und ständig aktualisierten WAF-Regeln schützt Myra auch vor Angriffen auf ungepatchte Systeme sowie auf nicht anders absicherbare Legacy-Anwendungen.

Faktor 3: Personalkosten vermeiden

Stellen Sie sich vor, Sie wollten ein eigenes Security Operations Center (SOC) betreiben und in Eigenregie für die erforderliche Sicherheit, Performance und rechtssichere Compliance Ihrer IT-Infrastruktur sorgen. Wie viele Fachleute mit welchen Gehältern müssten Sie einstellen, um sämtliche Aufgaben in den Bereichen Maintenance und Monitoring zu erfüllen? Abgesehen von dem Problem, in Zeiten des Fachkräftemangels überhaupt qualifiziertes Personal zu finden, kämen hier sehr hohe Personalkosten auf Sie zu. Mit der Auslagerung an einen Security-as-a-Service-Anbieter wie Myra können Sie diese Kosten vermeiden und zugleich ein erstklassiges Schutzniveau sicherstellen.

CapEx

Betrachten wir abschließend den dritten Parameter unserer Gleichung: Die Abkürzung CapEx steht für Capital Expenditures oder Capital Expenses und kann mit Investitionsausgaben übersetzt werden. CapEx beschreiben die Ausgaben eines Unternehmens für wichtige Güter, um die zukünftige Leistungsfähigkeit aufrechtzuerhalten oder noch zu steigern.

Gesamtbetriebskosten reduzieren

Die Gesamtbetriebskosten lassen sich unter anderem durch den Wechsel von On-Premises-Hardware zu einer skalierbaren Cloud-Lösung reduzieren, die keine zusätzliche Hard- oder Software erfordert. Der Myra Multi Cloud Load Balancer beispielsweise verringert den Traffic auf den Origin-Servern: Myra nimmt den gesamten Traffic an und liefert Antworten direkt aus dem Cache aus, ohne dass der Origin Server involviert wird. Das bedeutet weniger Traffic auf dem Origin und damit weniger Kosten.

Andere Komponenten der Myra-Plattform tragen zudem dazu bei, die Bandbreite zu verringern und die Kosten für den Traffic effektiv zu verringern: Mithilfe des High Performance CDNs lassen sich Inhalte schneller ausliefern und die letzte Meile zum Nutzer verkürzen. Der Origin Server wird damit entlastet, Kosten eingespart und die User Experience verbessert. Durch das Image Scaling wiederum wird die Auslieferung verschiedener Bildgrößen optimiert und damit schneller. Durch die derart verbesserte Auslastung der bestehenden Server-Landschaft entfällt in vielen Fällen die Notwendigkeit, weitere Server anzuschaffen, um die Leistungsfähigkeit beispielsweise eines Online-Shops weiter zu steigern.

6 www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/230227_Studie_Onlineshopping.html

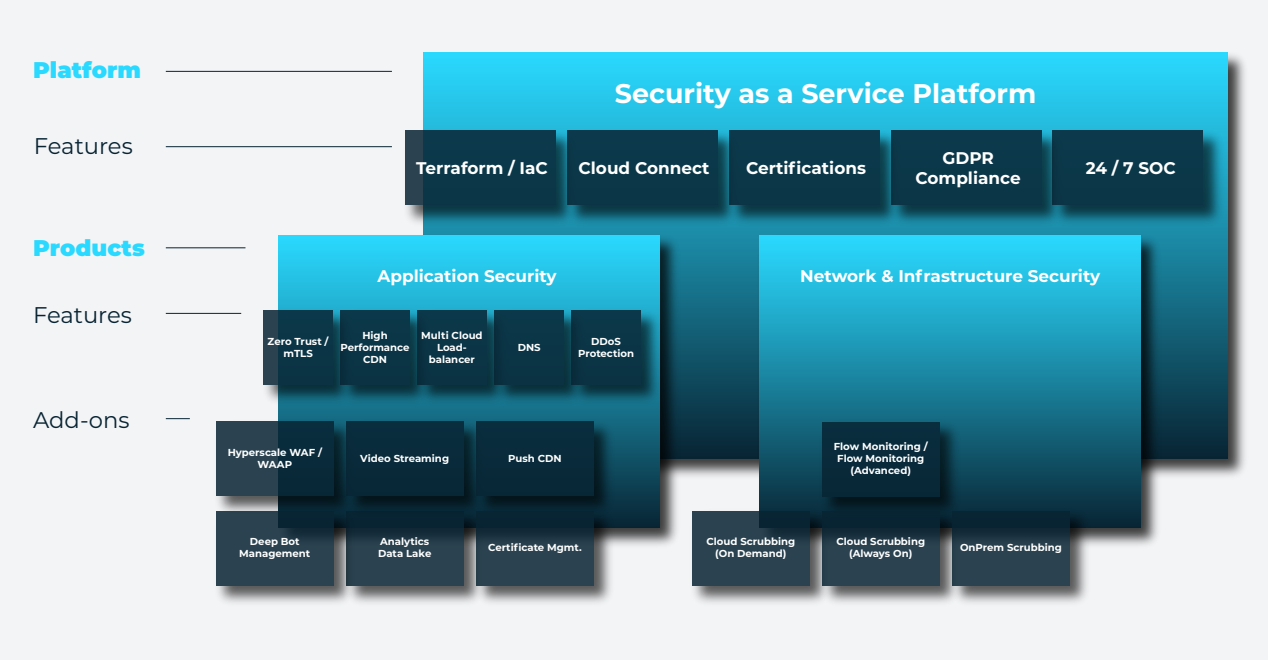
Fazit: Investition in IT-Sicherheit als aktive Kostenreduktion

Rufen wir uns nochmals die Formel vom Anfang ins Gedächtnis:

$$ROI = \frac{\Delta \text{ Revenue} + \Delta \text{ Cost} + \Delta \text{ Capex}}{\text{Invest}}$$

Schauen wir uns nun stellvertretend für den Parameter „Invest“ konkret die Investition in die Application-Security-Lösung von Myra an. Wie wir dargelegt haben, hat eine solche Lösung einen positiven Einfluss auf alle drei Parameter im Zähler. Der Invest sollte nicht höher sein als die Effekte, die man positiv auf Umsatz sowie Kosten und CapEx-Einsparungen bewertet.

Myra Cloud Platform



Mit den Security-as-a-Service-Lösungen von Myra minimieren Sie ungeplante Downtime, sorgen für eine schnelle Auslieferung Ihrer Website, schützen sich vor den Schäden, die bösartige Bots verursachen können und haben die Gewissheit, rechtssicher DSGVO-konform zu sein. Rufen Sie uns einfach an (+49 89 414141 – 345) oder schreiben Sie uns (info@myrasecurity.com), um einen Termin für eine unverbindliche kostenlose Schutzberatung zu vereinbaren.

Branchenführende Sicherheit, Performance und Compliance

- **BSI-KRITIS-qualifiziert:** Myra erfüllt als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister
- **Hochzertifizierte Qualität:** ISO 27001 auf Basis von IT-Grundschutz, PCI-DSS-zertifiziert, BSI-KRITIS-qualifiziert, BSI-C5-Testat Typ 2, DIN-EN-50600-zertifizierte Rechenzentren, Trusted Cloud, IDW PS 951 Typ 2 (ISAE 3402)
- **KRITIS-Cluster:** DSGVO- und IT-SiG-konforme, mehrfach georedundante Server-Infrastruktur in Deutschland
- **Made in Germany:** volle technische Kontrolle, permanente Weiterentwicklung, 24/7-Full-Service-Betreuung durch unser IT-Expertenteam im Security Operations Center

BSI-zertifizierte IT-Sicherheit

Die Myra-Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Zudem erfüllen wir als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz | Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600

Myra ist der Kompetenzpartner für den E-Commerce

Myra überwacht, analysiert und filtert schädlichen Internet-Traffic bevor virtuelle Angriffe einen realen Schaden anrichten. Unsere zertifizierte Security-as-a-Service-Plattform schützt Ihre digitalen Geschäftsprozesse vor vielfältigen Risiken wie DDoS-Attacken, Bot-Netzwerken und Angriffen auf Datenbanken.

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor bösartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihr Unternehmen. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

Kostenlose Schutzberatung anfordern →

Myra Security GmbH

Telefon +49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com