MYRA

CYBERSECURITY REPORT 2025

Resilienztest für die digitale Gesellschaft

In Zusammenarbeit mit:

zerobs

Vorwort

Das Jahr 2024 hat einmal mehr gezeigt, wie dynamisch und vielschichtig die aktuelle Bedrohungslandschaft im Cyberraum ist. Während wir einerseits eine Verschärfung der Lage beobachten konnten, zeichnete sich andererseits auch eine gewisse Entspannung ab. Diese Entwicklung verdeutlicht, dass die Bemühungen bei der Absicherung digitaler Geschäftsprozesse Wirkung zeigen. Gleichzeitig ist weiterhin größtmögliche Wachsamkeit und eine kontinuierliche Weiterentwicklung der Schutzmaßnahmen geboten.

Der vorliegende Report behandelt vielfältige Herausforderungen: von der steigenden Zahl und Komplexität von DDoS-Angriffen über die Verwundbarkeit digitaler Lieferketten bis hin zu den Risiken im Kontext demokratischer Wahlen. Besonders besorgniserregend ist die wachsende Bedrohung kritischer Infrastrukturen und des öffentlichen Sektors, die das Fundament unseres gesellschaftlichen Lebens bilden.

Trotz der aktuellen Entwicklung und der ernstzunehmenden Lage besteht durchaus Grund zur Zuversicht. Die technischen Fortschritte in der Automatisierung und der Einsatz künstlicher Intelligenz (KI) eröffnen neue Möglichkeiten für eine effizientere und präzisere Cyberabwehr. Gleichzeitig beobachten wir eine wachsende Bereitschaft von Behörden und Unternehmen, verstärkt in ihre digitale Resilienz zu investieren.

Um unsere Gesellschaft nachhaltig und effizient vor Cyberbedrohungen zu schützen, bedarf es jedoch eines holistischen Ansatzes. Dieser umfasst nicht nur technologische Maßnahmen, sondern auch die grundlegende Sensibilisierung für Cybersicherheit auf allen Ebenen. Regulatorische Frameworks wie NIS-2, der Cyber Solidarity Act oder der Cyber Resilience Act bilden dabei wichtige Eckpfeiler für einen EU-weiten Schutzschild.

Die Herausforderungen mögen groß sein, doch die Bündelung von Expertisen und Ressourcen sowie die kontinuierliche Weiterentwicklung von Schutztechnologien bieten das Potenzial für eine resiliente digitale Zukunft. Lassen Sie uns diese Aufgabe mit Entschlossenheit und Optimismus angehen – für eine sichere und prosperierende digitale Gesellschaft in Europa.

Christof Klaus
Director Global Network Defense
bei Myra Security

Inhalt

Vorwort ... 2
Executive Summary ... 3
Bedrohungslage zwischen Allzeithoch und Entspannung ... 7
Cyberhotspots: KRITIS und Public Sector ... 8
Cyberrisiken im Kontext der Bundestagswahl 2025 ... 11
DDoS Resiliency Score macht Schutz messbar ... 14
Automatisierung trifft Präzision: Über die Herausforderungen effizienter Cyberabwehr ... 16
Quellen und Referenzen ... 18

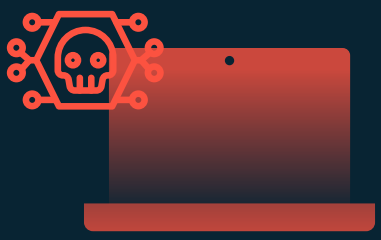
Executive Summary

Dynamische Cyberbedrohungslage

In der ersten Jahreshälfte 2024 wurde ein signifikanter Anstieg von schädlichen Traffic-Strömen um 53 % im Vergleich zum Vorjahr verzeichnet, mit einem Höhepunkt im Juli. Ab diesem Zeitpunkt nahm die Anzahl der Angriffe schrittweise ab und lag ab Oktober unter dem Vorjahreswert. Während geopolitische Konflikte und gesellschaftliche Großereignisse wie Olympia 2024 oder das Superwahljahr als Katalysator fungierten, trugen erfolgreiche Operationen internationaler Ermittlungsbehörden zur Entschärfung der Lage bei. Trotz der Trendwende wurde über das gesamte Jahr hinweg ein Anstieg schädlicher Requests um 25 % ermittelt.

Herausforderung Lieferkette

Die weltweiten Ausfälle infolge des fehlgeschlagenen Crowdstrike-Updates sowie der in letzter Sekunde vereitelte Backdoor-Angriffsversuch auf XZ-utils haben die Anfälligkeit digitaler Infrastruktur aufgezeigt. Speziell bei robust abgesicherten IT-Systemen ist ein Angriff des eigentlichen Ziels über den Umweg einer Attacke auf externe Dienstleister oft der effizientere Weg für Cyberkriminelle.

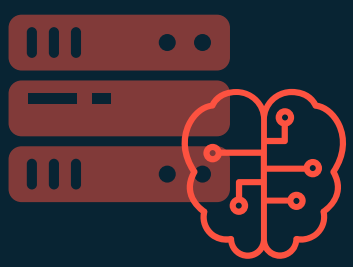


Kostentreiber Cyberkriminalität

Wenn Frequenz und Intensität von Angriffen auf digitale Infrastrukturen zunehmen, treibt das auch die Schäden und die damit einhergehenden Kosten in die Höhe. Deutschlandweit wird aktuell mit Cybercrime-bedingten Schäden in Höhe von 178,6 Milliarden Euro pro Jahr gerechnet.

KI: von der Vision zur Praxis

Der Hype um künstliche Intelligenz (KI) in der Cybersicherheit weicht 2024 einer pragmatischeren Sichtweise mit einem zunehmenden Fokus auf konkrete messbare Vorteile. Diese lassen sich speziell bei der Automatisierung routinemäßiger Aufgaben wie der Angriffserkennnug verorten – hier beschleunigt der KI-Einsatz die Identifikation von Gefahren in den meisten Fällen um bis zu 10 %.

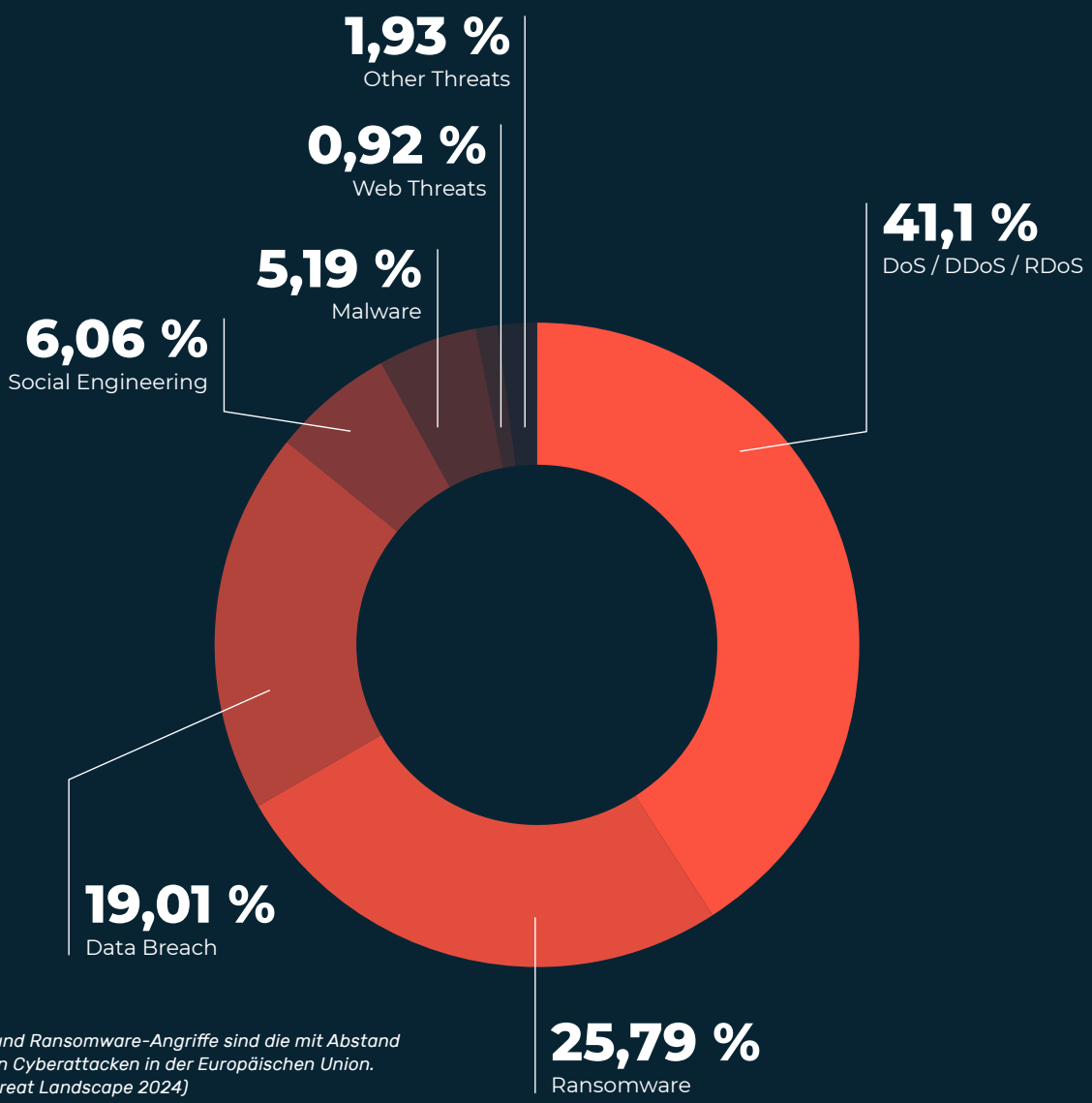


Im Jahr 2024 hat sich die Cybersicherheitslage insgesamt dynamisch entwickelt. Nachdem es zunächst zu einer Verschärfung kam, war im weiteren Verlauf eine allmähliche Abmilderung zu beobachten. Konkret kam es im ersten Halbjahr zu einem deutlichen Anstieg schädlicher Traffic-Ströme um 53 % im Vergleich zum Vorjahr. Dabei handelte es sich primär um DDoS-Angriffe sowie um Bot-basierte Attacken auf Schwachstellen in Online-Anwendungen und Datenbanken.

Diese Zunahme ist auf mehrere Faktoren zurückzuführen, darunter geopolitische Spannungen wie der Israel-Gaza-Konflikt, der anhaltende Ukraine-Krieg und die Taiwan-Frage. Diese Faktoren führten zu verstärktem Hacktivismus und Aktivitäten staatlich unterstützter Akteure. Zusätzlich boten Großereignisse wie die Olympischen Spiele in Paris und die Wahlen in Russland, Indien, der EU, den USA sowie die Landtagswahlen in Deutschland Angriffsflächen für orchestrierte Cyberattacken.

Die meisten Angriffe verzeichneten die Systeme von Myra im Juli. Nach diesem Höhepunkt folgte eine Trendwende: Ab August waren die Angriffe im Monatsverlauf rückläufig. Im Oktober lag die Anzahl der blockierten Requests erstmals unter dem Vorjahreswert. Diese positive Entwicklung lässt sich mitunter auf erfolgreiche Operationen internationaler Ermittlungsbehörden zurückführen, die zur Abschaltung zentraler Cybercrime-as-a-Service-Plattformen führten. Ungeachtet der Trendwende lässt sich über das gesamte Jahr hinweg ein Anstieg schädlicher Anfragen um 25 % beobachten. In der Gesamtbetrachtung hat sich die Risikolage im Bereich schädlicher Traffic-Ströme damit wie in den vergangenen Jahren verschärft.

Cyberbedrohungslage Europa: Primäre Angriffsvektoren nach Anzahl von Vorfällen



DDoS-Attacken und Ransomware-Angriffe sind die mit Abstand meist gemeldeten Cyberattacken in der Europäischen Union. (Quelle: ENISA Threat Landscape 2024)

Hintertüren und Pannen: die wachsenden Risiken digitaler Lieferketten

Die Ereignisse von 2024 zeigen, dass selbst gut geschützte IT-Infrastrukturen durch Schwachstellen in digitalen Lieferketten gefährdet sind. Angreifer nutzen dies zunehmend aus, indem sie weit verbreitete Software-Bibliotheken ins Visier nehmen.

Ein bemerkenswertes Beispiel hierfür war der Backdoor-Angriffsversuch auf XZ-utils, eine verbreitete Sammlung von Archivierungsprogrammen für Linux. Diese Supply-Chain-Attacke wurde zufällig am 28. März 2024 entdeckt, als ein PostgreSQL-Entwickler ungewöhnliche CPU-Auslastungen bei SSH-Verbindungen bemerkte.

Die Angreifer hatten über drei Jahre das Open-Source-Projekt infiltriert, um Schadcode einzuschleusen, der Fernzugriff ermöglichte. Die Schwachstelle erhielt die höchste CVSS-Bewertung (Common Vulnerability Scoring System) von 10. Die Komplexität und langfristige Planung deuten auf staatlich unterstützte Akteure hin.

Risiken für digitale Lieferketten gehen aber nicht nur von böswilligen Angriffen aus, auch fehlerhafte Software Patches stellen ein Problem dar. Die globalen Ausfälle von Flughäfen, Krankenhäusern, Banken, Behörden und zahllosen Unternehmen im Rahmen der Crowdstrike-Panne vom 19. Juli verdeutlichen dies eindrucksvoll.

Weltweit hat das fehlerhafte Update für den Ausfall von etwa 8,5 Millionen Windows-Systemen gesorgt. Die geschätzten Gesamtkosten des Ausfalls belaufen sich auf etwa 5,4 Milliarden US-Dollar für die Fortune-500-Unternehmen in den USA. Weltweit wird der Gesamtschaden auf etwa 15 Milliarden US-Dollar geschätzt.

Cyberrisikolage Deutschland

Im Durchschnitt erfahren Unternehmen

49 Cyberattacken pro Jahr

Die Folgen

25 % erleiden Schäden über 500.000 €
46 % verlieren Kunden
47 % haben Probleme bei der Kundenakquise

Quelle: Hiscox

> *Cybersicherheit wird immer mehr vom abstrakten Kostenfaktor zum konkreten Verkaufsargument avancieren, denn nur wenn ich als Unternehmen hinreichend sichere Prozesse habe, können sich die Kunden auch auf meine Leistungsfähigkeit verlassen.*

Prof. Dr. Dennis-Kenji Kipker
Research Director cyberintelligence.institute
und Myra Advisory Board Member

Cyberkriminalität treibt Kosten in die Höhe

Die Verschärfung der Bedrohungslage über die vergangenen Monate lässt sich ebenso anhand der gestiegenen Schadenssummen nachvollziehen. So verzeichnet das Bundeskriminalamt (BKA) einen alarmierenden Anstieg von Schäden durch organisierte Cyberkriminalität. Die Schadenssumme hat sich im Vergleich zum Vorjahr nahezu verdreifacht und erreichte 1,7 Milliarden Euro. Damit macht Cybercrime fast zwei Drittel der Gesamtschäden durch Organisierte Kriminalität aus, die sich auf 2,7 Milliarden Euro belaufen – mehr als doppelt so viel wie im Vorjahr. BKA-Präsident Holger Münch betont: „Die Bekämpfung der Organisierten Kriminalität bleibt ein zentraler Schwerpunkt unserer Arbeit. Sie verursacht hohe Schäden und stellt durch Einflussnahmen und Gewalt eine erhebliche Bedrohung für Staat, Wirtschaft und Gesellschaft dar.“ [1]

Eine breitere Betrachtung des Schadensausmaßes liefert der Branchenverband Bitkom. Dessen Untersuchungen ergaben, dass sich die durch Cybersicherheitsvorfälle entstandenen Schäden für die deutsche Wirtschaft auf 178,6 Milliarden Euro jährlich belaufen.[2]

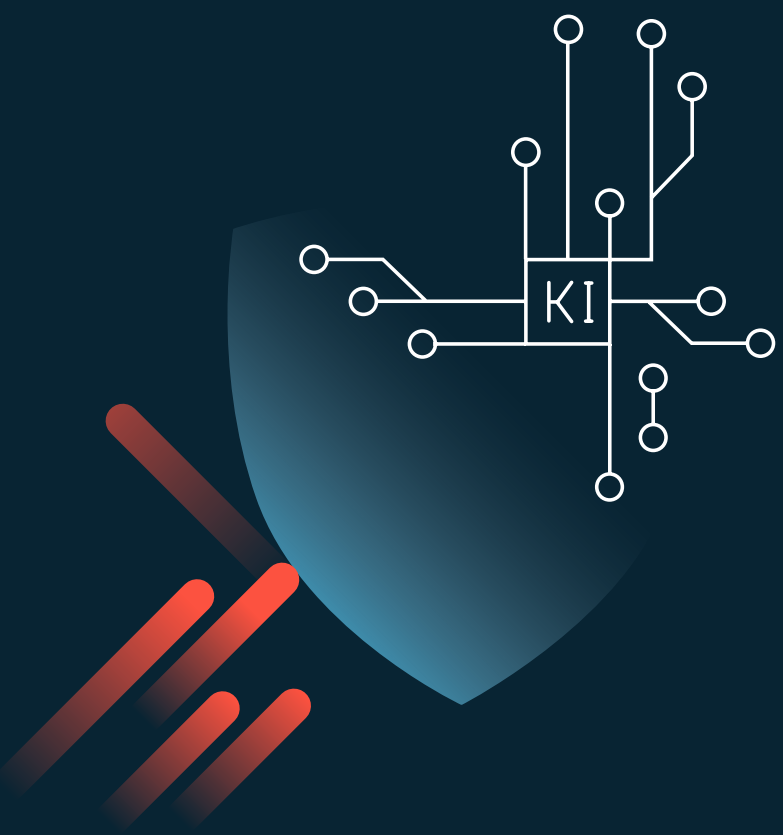
Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) berichtet von einer ähnlichen Entwicklung. Demnach stieg die Anzahl der bei Versicherern gemeldeten Cyberangriffe zuletzt um 19 % auf etwa 4.000 Fälle. Die Versicherungsgesellschaften leisteten hierfür Zahlungen in Höhe von rund 180 Millionen Euro, was einer Steigerung von 50 % gegenüber dem Vorjahr entspricht. Der durchschnittliche Schaden pro Angriff belief sich auf 45.370 Euro.[3]

KI-Konsolidierung in der Cybersicherheit

Indessen weicht der anfängliche Hype um künstliche Intelligenz (KI) in der Cybersicherheit im Jahr 2024 einer nüchterneren Betrachtung. Zwar ist weiterhin jeder zweite IT-Entscheidende der Meinung, dass KI die IT-Sicherheit seiner Organisation maßgeblich verbessern kann, doch liegt der Fokus nun zunehmend auf konkreten Business Cases, die messbare Vorteile liefern.[4] Die Automatisierung routinemäßiger Aufgaben kristallisiert sich als größter Vorteil von KI in der Cybersicherheit heraus. Der Einsatz intelligenter Algorithmen ermöglicht es Unternehmen, große Datenmengen in kürzester Zeit zu analysieren und so Angriffsmuster frühzeitig zu identifizieren. 9 von 10 Organisationen haben durch den Einsatz von KI die Angriffserkennung um bis zu 10 % beschleunigt.[5] Die dadurch eingesparten Kapazitäten können Sicherheitsteams darauf verwenden, sich mit komplexeren Aufgaben zu befassen. Angesichts des anhaltenden Fachkräftemangels in der IT-Sicherheit bietet KI hier eine willkommene Entlastung.
In Deutschland berichten 62 % der Organisationen von Personalengpässen im Bereich Cybersicherheit, konkret fehlen aktuell rund 120.000 IT-Sicherheitsfachleute.[6]

> *„Die sabotierten Präsidentschaftswahlen in Rumänien liefern die Blaupause: Ein KI-Botnetz reicht aus, um unsere Demokratie vollständig zu untergraben. Die Zeit der Warnungen ist vorbei – entweder wir rüsten unsere digitale Resilienz jetzt auf oder wir verlieren die Kontrolle über unsere demokratischen Prozesse."*

Sergej Epp
CISO bei Sysdig und
Myra Advisory Board Member



Auf der anderen Seite nutzen Cyberkriminelle KI-Technologie, um Angriffe zu verschleiern und Sicherheitslücken in kürzester Zeit auszunutzen. Dies setzt IT-Sicherheitsteams zunehmend unter Druck, verfügbare Patches schnellstmöglich zu installieren und die Angriffsfläche bei bekannt gewordenen Schwachstellen zu reduzieren. Entsprechend gehen 8 von 10 Unternehmen in Deutschland davon aus, dass die breite Verfügbarkeit von KI die Bedrohungslage für die Wirtschaft nachhaltig verschärft hat.[7]

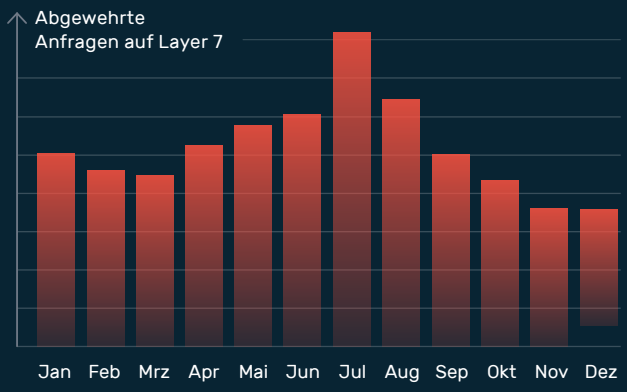
Die hohe Dynamik in diesem Technologiebereich stellt auch die europäische Digitalpolitik vor enorme Herausforderungen. Einerseits gilt es, Innovationen zu fördern und die Wettbewerbsfähigkeit europäischer Unternehmen zu stärken. Andererseits müssen Risiken effektiv eingedämmt und ethische Standards gewahrt werden. Die Umsetzung des von der EU-Kommission auf den Weg gebrachten AI Act bietet hier eine Gelegenheit, diese Ziele sukzessiv und strukturiert zu verfolgen.

Bedrohungslage zwischen Allzeithoch und Entspannung

Die Bewältigung von Cybervorfällen, die durch schädlichen Traffic hervorgerufen werden, stellt für immer mehr Organisationen in Deutschland und Europa eine immense Herausforderung dar. 4 von 10 Cybervorfällen in Europa (41,1 %) sind auf DDoS-Angriffe zurückzuführen, gefolgt von Ransomware-Attacken mit 27,3 %. [8]

Die Analysen aus dem Myra SOC (Security Operations Center) unterstreichen diesen Trend. Über den gesamten Jahresverlauf war hier eine Zunahme schädlicher Anfragen um rund 25 % festzustellen. Insbesondere in der ersten Jahreshälfte bis einschließlich Juli war ein deutliches Wachstum zu verzeichnen. Die schädlichen Traffic-Ströme setzen sich zusammen aus DDoS-Angriffen, Bot-Attacken und schädlichen Zugriffsversuchen auf Datenbanken via Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) oder SQL Injection.

Angriffsaktivität 2024

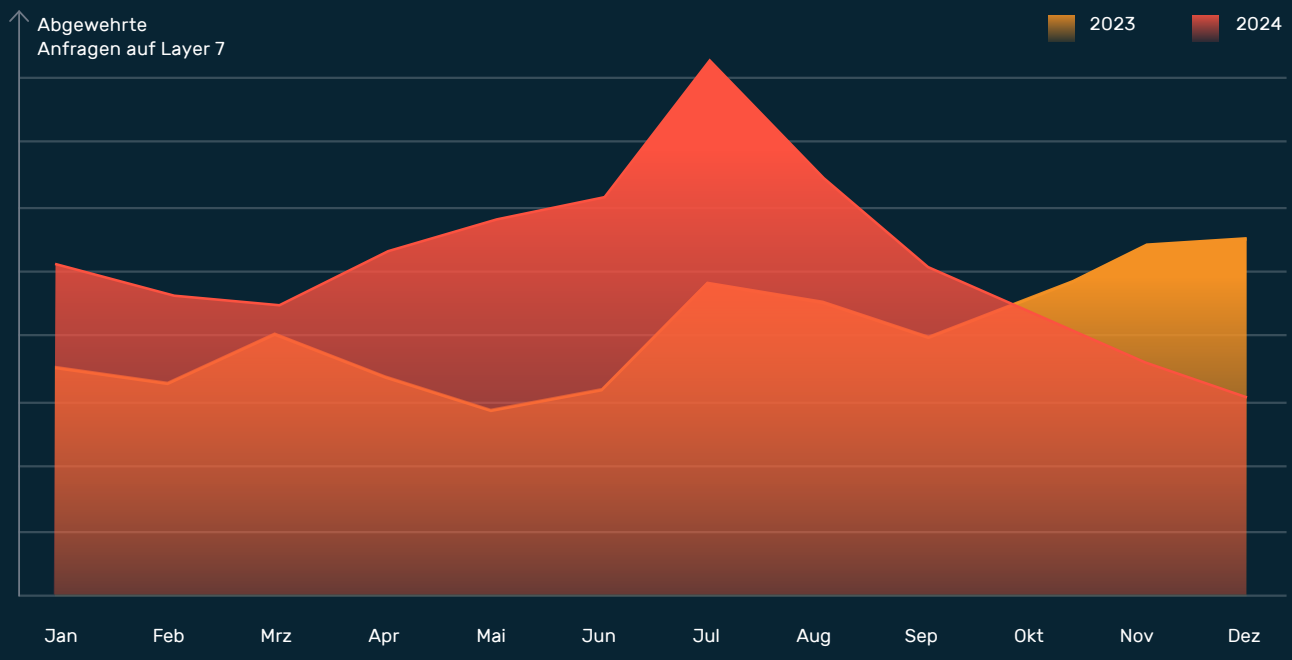


Schädliche Traffic-Ströme auf Applikationsebene erreichten zur Jahresmitte 2024 ihren Höchststand.

Der Juli 2024 markiert den mitigationsintensivsten Monat seit Beginn der Auswertung. Im Zeitraum Januar bis Juli stieg die Zahl der abgewehrten Requests um 53 % im Vergleich zum Vorjahr. Nach Juli lässt sich hingegen eine Trendwende beobachten. Ab hier nahm die Anzahl der Angriffe in der monatlichen Betrachtung schrittweise ab und lag seit Oktober unterhalb des Vorjahreswertes. Im Vergleich zu den intensiven Sommermonaten entspannte sich die Lage zum Jahresausgang zusehends.

Die beobachtete Entwicklung der Cyberangriffe im Jahr 2024 lässt sich durch eine Kombination verschiedener Faktoren erklären. Einerseits war die erste Jahreshälfte stark durch geopolitische Konflikte geprägt, die eine Zunahme von Hacktivismus und der Aktivität staatlich unterstützter Akteure mit sich brachten. Zu nennen wären hier etwa der Israel-Gaza-Konflikt, der anhaltende Ukraine-Krieg sowie die Taiwan-Frage.

Jahresvergleich



Im Gesamtjahr 2024 verzeichneten die Abwehrsysteme von Myra einen Anstieg der schädlichen Anfragen um 25 %. Im Juli setzte eine Trendwende ein, seither sind die Angriffszahlen rückläufig – ab Oktober lagen die Werte sogar unter denen des Vorjahres.

Zusätzlich boten gesellschaftliche Großereignisse wie die Olympischen Spiele in Paris sowie die Wahlen in Russland, Indien, der EU, den USA und die Landtagswahlen in Sachsen, Thüringen und Brandenburg Anlass für orchestrierte Angriffe. Dabei ist zu beachten, dass Cyberakteure ihre Angriffskampagnen meist schon Monate vor dem eigentlichen Termin des jeweiligen Zielereignisses starten – insbesondere bei Wahlen, um mittels Desinformation und Verunsicherung Einfluss zu nehmen (mehr hierzu im Kapitel „Cyberrisiken im Kontext der Bundestagswahl 2025" auf S.11 ff.).

Ebenfalls von Gewicht ist in diesem Zusammenhang das erfolgreiche Vorgehen internationaler Ermittlungsbehörden gegen professionelle Cyberakteure. So wurden etwa im Mai bei einer global koordinierten Operation gegen Botnetze über 100 Server und mehr als 2.000 Domains abgeschaltet, die mit der Verbreitung von Schadsoftware im Zusammenhang standen.[9] Weitere erfolgreiche Operationen wie „PowerOFF" führten im Jahresverlauf zur Schließung von „Digitalstress", des weltweit aktivsten Underground-Marktplatzes für DDoS-Dienste, sowie zur Beschlagnahme von 27 der meistgenutzten Stresser-Dienste, über die Cyberkriminelle ohne viel Aufwand Überlastungsattacken buchen konnten.[10]

Die gefährlichsten Software-Schwachstellen 2024
(MITRE CWE Top 25)

1	Cross-site Scripting
2	Out-of-bounds Write
3	SQL Injection
4	Cross-site Request Forgery (CSRF)
5	Path Traversal

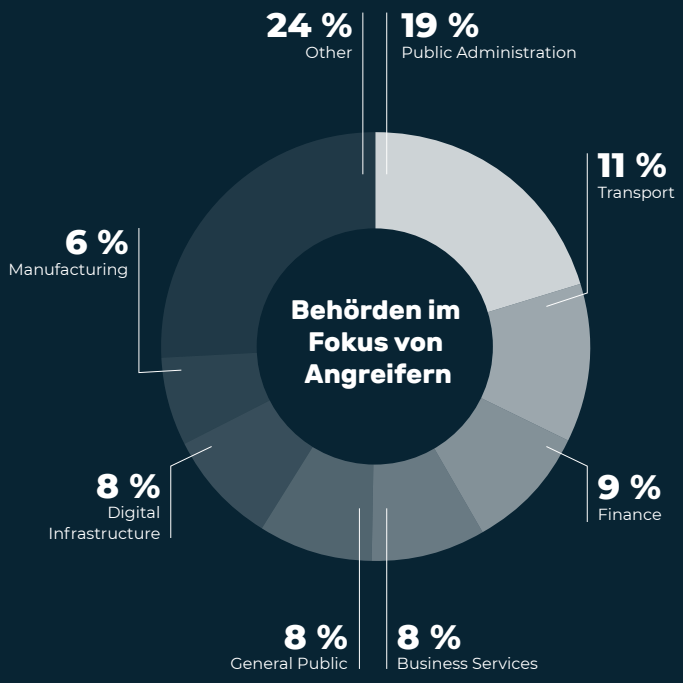
Die Liste basiert auf der Analyse von mehr als 31.000 CVE-Einträgen und dient als Leitfaden für Entwickler und Sicherheitsteams, um kritische Sicherheitsrisiken zu priorisieren und zu adressieren.

Cyberhotspots: KRITIS und Public Sector

Unterdessen hat sich die risikobehaftete Bedrohungslage für Kritische Infrastrukturen (KRITIS) und Einrichtungen der öffentlichen Verwaltung auch im Jahr 2024 keineswegs entspannt – im Gegenteil. Die Ausbreitung von Hacktivismus und die zunehmenden Aktivitäten politisch motivierter und staatlich unterstützter Cyberakteure stellen insbesondere diese Sektoren vor zusätzliche Herausforderungen.

Da Vorfälle bei Behörden oder kritischen Einrichtungen in der Regel schnell publik werden, eignen sich diese Organisationen aus Angreifersicht als Zielscheibe, um Schaden anzurichten und Verunsicherung in der Gesellschaft zu stiften. Die betroffenen Organisationen sind sich dieser Situation durchaus bewusst: 9 von 10 KRITIS-Betreibern gehen aktuell von einer Verschärfung der Bedrohungslage aus (87 %).[11]

Cyberbedrohungslage Europa: Zielsektoren nach Anzahl von Vorfällen



Verwaltungsbehörden im Fokus von Cyberkriminellen: Jeder fünfte Cyberangriffe in Europa richtet sich gegen eine Organisation aus dem öffentlichen Sektor. (Quelle: ENISA Threat Landscape 2024)

KRITIS: steigende Fallzahlen

In den ersten drei Quartalen des Jahres 2024 wurden dem BSI bereits 612 Vorfälle bei KRITIS-Betreibern gemeldet. Diese hohe Zahl unterstreicht die Dringlichkeit, Schutzmaßnahmen kontinuierlich zu verbessern und an neue Bedrohungsszenarien anzupassen. Besonders besorgniserregend sind dabei Angriffe oder Vorfälle, die zu Ausfällen oder Beeinträchtigungen kritischer Dienstleistungen führen.

Ein Beispiel für die Verwundbarkeit digitaler Infrastruktur war der globale Ausfall von Windows-Systemen durch ein fehlerhaftes Crowdstrike-Update im Juli 2024. Der US-Anbieter von Cybersicherheitslösungen hatte fehlerhafte Änderungen am hauseigenen Produkt „Falcon Sensor" vorgenommen, die zu Systemausfällen in Windows-Umgebungen führten.

Aufgrund des Vorfalls mussten tausende Flüge abgesagt, geplante Operationen in Krankenhäusern vertagt und unzählige Digitaldienste über Stunden hinweg deaktiviert bleiben. Davon betroffen waren etwa Banken, Einzelhändler, Medien- und Telekommunikationsunternehmen sowie auch Regierungsbehörden.

Der Crowdstrike-Vorfall zeigt deutlich, wie wichtig redundant abgesicherte Systeme und digitale Souveränität in der heutigen IT-Landschaft sind. Einen Single-Point-of-Failure dürfen sich Betreiber kritischer Infrastrukturen nicht leisten – insbesondere, wenn dieser außerhalb der eigenen Einflussnahme in der digitalen Lieferkette angesiedelt ist.

Der Crowdstrike-Ausfall 2024 in Zahlen und Fakten:

Zeitpunkt:
19. Juli 2024

Betroffene Systeme:
8,5 Millionen Windows-Geräte

Dauer des Ausfalls betroffener Dienstleistungen:
ca. 10 Stunden

Geschätzter Schaden:
über 15 **Milliarden US-Dollar**

Flugausfälle:
5.078 gestrichene Flüge weltweit

Betroffene Systeme in deutschen Unternehmen: **Ein Drittel aller PCs, die Hälfte aller Server**

62 %

der befragten Unternehmen in Deutschland waren direkt betroffen

48 %

der befragten Unternehmen in Deutschland waren indirekt über Partner betroffen

Quellen: BSI, Bitkom, Reuters/Parametrix

Öffentliche Verwaltung im Visier

Für Hacktivisten und politisch motivierte Cybergruppen sind DDoS-Attacken das Mittel der Wahl, um öffentlichkeitswirksam Cybervorfälle zu provozieren. In Europa ist der öffentliche Sektor mit Abstand am stärksten von Überlastungsangriffen betroffen: 33 % aller gemeldeten DDoS-Attacken zielen auf die Webseiten und Dienste von Behörden. Bei 41 % der DDoS-Attacken wird eine politische Motivation oder aktivistische Agenda vermutet, beispielsweise im Zusammenhang mit dem Krieg in der Ukraine. Bemerkenswert ist zudem, dass 56,8 % der untersuchten DDoS-Angriffe zu einem vollständigen Ausfall des Ziels führten.[12, 13]

Cybervorfälle bei Behörden und Kommunen

Auswahl publik gewordener Cybervorfälle im öffentlichen Sektor für das Jahr 2024.

Das Jahr 2024 war europaweit von mehreren Wellen orchestrierter Angriffskampagnen geprägt. Zu größeren Angriffswellen kam es im März in Frankreich, wo die Angreifer nach eigenen Angaben 17.000 IP-Adressen und Geräte sowie mehr als 300 Domains lahmgelegt haben.[14] Größere Kampagnen gab es auch in der Schweiz im Umfeld der Ukraine-Friedenskonferenz im Juni und in Österreich im Vorfeld der Nationalratswahlen im September.[15] Im Oktober verlagerten sich die Angriffe auf Belgien als mögliche Reaktion auf versprochene Waffenlieferungen an die Ukraine.[16]

Die meisten Angriffe richteten sich gegen (Polizei-) Behörden und Organisationen der öffentlichen Verwaltung, gefolgt von Finanzinstituten und dem Transportwesen[17] – so auch in Deutschland. Hierzulande kam es in den Monaten März bis Juni sowie Oktober bis Dezember zu größeren Angriffswellen. Hinter den DDoS-Attacken standen zumeist einschlägige Cybergruppen wie NoName057(16), Anomyous Sudan oder Cyber Army Russia.

Aufgrund des anhaltenden Trends zu Cybercrime-as-a-Service sind DDoS-Angriffe für die Akteure mit geringem Aufwand und niedrigen Kosten verbunden. Dieser Umstand ermöglicht sowohl eine hohe Frequenz als auch einen vergrößerten Umfang der Angriffe. Auf der Seite der betroffenen Organisationen hingegen ist eine Abwehr nur mit dedizierten Schutzsystemen auf den relevanten Netzwerkschichten möglich. Im Fall von groß angelegten DDoS-Kampagnen lässt sich daher immer dasselbe Resultat beobachten: geschützte Umgebungen halten den Angriffen stand, während ungeschützte zusammenbrechen – mit sämtlichen Konsequenzen, die sich daraus ergeben.

NIS-2 ausgebremst

Als Reaktion auf die anhaltend angespannte Cyberbedrohungslage hat die EU-Kommission zum horizontalen Schutz kritischer Einrichtungen die NIS-2-Richtlinie auf den Weg gebracht. Allerdings verzögert sich deren Umsetzung, die für den 17. Oktober 2024 angedacht war, in vielen Mitgliedstaaten, darunter auch Deutschland. Aufgrund des Bruchs der Ampelkoalition rechnen Fachleute mit einem Start von NIS-2 in Deutschland nunmehr erst ab Herbst 2025. Diese Verzögerung ist bedauerlich, da die Richtlinie darauf abzielt, das Cybersicherheitsniveau in der gesamten Europäischen Union zu erhöhen und die Resilienz kritischer Sektoren zu stärken.

Dennoch bereiten sich viele Unternehmen bereits auf die kommenden Anforderungen vor. Untersuchungen von Branchenverbänden belegen, dass knapp die Hälfte der befragten Unternehmen bereits Maßnahmen ergriffen hat, um ihre Cybersicherheit gemäß der neuen Richtlinie sicherzustellen – am wachsenden Bewusstsein für die Brisanz und Dringlichkeit des Themas seitens der Wirtschaft mangelt es nicht.

EU-Regelungen für mehr Cybersicherheit

Während die NIS-2-Richtlinie in Deutschland und vielen anderen EU-Mitgliedstaaten noch in der Umsetzungsphase steckt, versprechen der Cyber Solidarity Act (CSA) und der Cyber Resilience Act (CRA) in naher Zukunft die Cybersicherheit in der Europäischen Union zu stärken.

Die CSA-Verordnung regelt den Umgang und die Reaktion der Mitgliedstaaten im Kontext schwerwiegender Cybervorfälle. Ziel der Verordnung ist es, die Zusammenarbeit zwischen den EU-Ländern bei größeren Cyberangriffen zu verbessern sowie schnelle und effektive Gegenmaßnahmen zu ermöglichen.

Parallel dazu legt der Cyber Resilience Act neue Cybersicherheitsstandards für Produkte mit digitalen Komponenten fest und verpflichtet Hersteller, die Sicherheit während des gesamten Lebenszyklus zu gewährleisten.

Zusammen schaffen diese Rechtsvorschriften einen robusten Rahmen für den Schutz kritischer Infrastrukturen, fördern die Zusammenarbeit zwischen den EU-Mitgliedstaaten und erhöhen so die Widerstandsfähigkeit des öffentlichen Sektors sowie der Wirtschaft gegenüber Cyberangriffen.

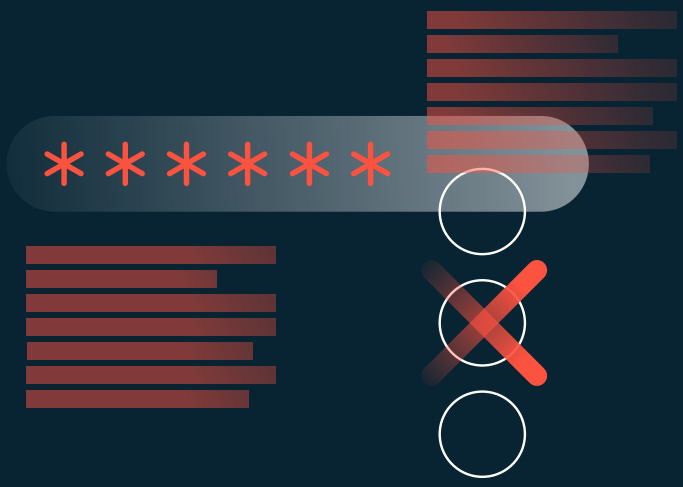
Cyberrisiken im Kontext der Bundestagswahl 2025

Mitte Februar 2025 soll der Deutsche Bundestag neu gewählt werden. Diese Wahlen gilt es zuverlässig und effizient vor Bedrohungen zu schützen. Die vergangenen Jahre haben gezeigt, dass Wahlprozesse grundsätzlich ein bevorzugtes Ziel von politisch beziehungsweise ideologisch motivierten Cyberakteuren darstellen.
So ergaben etwa veröffentlichte Untersuchungen des rumänischen Geheimdienstes, dass die Wahlinfrastruktur des Landes im Kontext der Präsidentschaftswahlen Ziel von mehr als 85.000 Cyberangriffen war.[18] Aufgrund dieser Einflussnahme auf den Wahlprozess sah sich das oberste Gericht Rumäniens dazu gezwungen, die erste Runde der Präsidentschaftswahlen für ungültig zu erklären.[19] Ähnliche Angriffsmuster ließen sich auch bei den Wahlen in der Republik Moldau sowie in Österreich (siehe Mitigation Case auf S. 13) feststellen.[20]

In Deutschland warnte indessen Ende November 2024 das Bundesamt für Verfassungsschutz vor Risiken durch die Einflussnahme anderer Staaten auf die anstehende Bundestagswahl. „Einzukalkulieren sind Aktionen der Desinformation und Diskreditierung, Cyberangriffe sowie Spionage und Sabotage", teilten die Verfassungsschützer mit. „Sie zielen darauf ab, im Verborgenen und unter Vortäuschung falscher Tatsachen Einfluss auf Entscheidungs- und Funktionsträger in anderen Staaten auszuüben, aber auch in den freien Meinungs- und Willensbildungsprozess einzugreifen."[21]

Zwar laufen die Wahlen in Deutschland per se weitestgehend analog ab, doch die damit im Zusammenhang stehenden Infrastrukturen von Ämtern, Behörden, Parteien und deren Dienstleister bieten sehr wohl Angriffsfläche. Die Methoden fallen dabei mannigfaltig aus.

Mittels klassischer Schadsoftware wie Ransomware-Trojanern oder Wiperware können wichtige Daten rund um den Wahlvorgang wie etwa Wählerregistrierungsdaten unzugänglich gemacht oder zerstört werden. DDoS-Attacken und Website Defacements untergraben wiederum das Vertrauen in den Wahlprozess, besonders wenn sie die Übermittlung und Anzeige von Wahlergebnissen beeinträchtigen oder manipulieren. Supply-Chain-Angriffe können dafür eingesetzt werden, um über Schwachstellen bei Zulieferern die digitale Infrastruktur im Zusammenhang mit der Wahl zu sabotieren. Durch den Einsatz von Social Engineering und Phishing gelangen Cyberakteure an sensible Informationen, die sie etwa für Desinformationskampagnen nutzen.[22]



> *„Wir wollen definitiv sicherstellen, dass nicht nur die Wahl sicher ist, sondern dass auch das Vertrauen der Menschen in die Wahl gegeben ist."*
>
> BSI-Präsidentin Claudia Plattner

Darüber hinaus gewinnen hybride Bedrohungen wie FIMI (Foreign Information Manipulation and Interference) an Bedeutung. Untersuchungen des Europäischen Auswärtigen Dienstes (EEAS) ergaben, dass FIMI-Kampagnen plattformübergreifend über viele unterschiedliche Kanäle koordiniert werden, um so die Illusion einer authentischen Diskussion und eines Interesses zu erzeugen und um die Herkunft von FIMI-Inhalten zu verschleiern. Bei den 750 untersuchten Vorfällen waren mehr als 4.000 Kanäle 9.800-mal aktiv. Dabei handelte es sich sowohl um Websites sowie auch um Social-Media-Profile, -Gruppen und -Seiten. Die am häufigsten beteiligten Plattformen waren Telegram und X (ehemals Twitter). FIMI-Aktivitäten wurden jedoch auf praktisch allen anderen großen, neuen und Nischenplattformen beobachtet.[23]

Die Erstellung von Inhalten für FIMI-Aktivitäten sowie die Distribution innerhalb sozialer Netze erfolgt zunehmend unter Zuhilfenahme von KI. Die breite Verfügbarkeit von Large-Language-Modellen (LLMs) und KI-basierten Bots bilden hier Katalysatoren, durch die sich Desinformationskampagnen in kürzester Zeit hochskaliert verbreiten lassen. Ebenso problematisch gestaltet sich die steigende Zahl von Deepfakes. Dabei handelt es sich um mittels KI manipulierte Videos, Fotos und Tonaufnahmen, die kaum von Original-Inhalten zu unterscheiden sind – in der Praxis ist lediglich einer von zehn Nutzenden zuversichtlich, Deepfakes zu erkennen.[24]

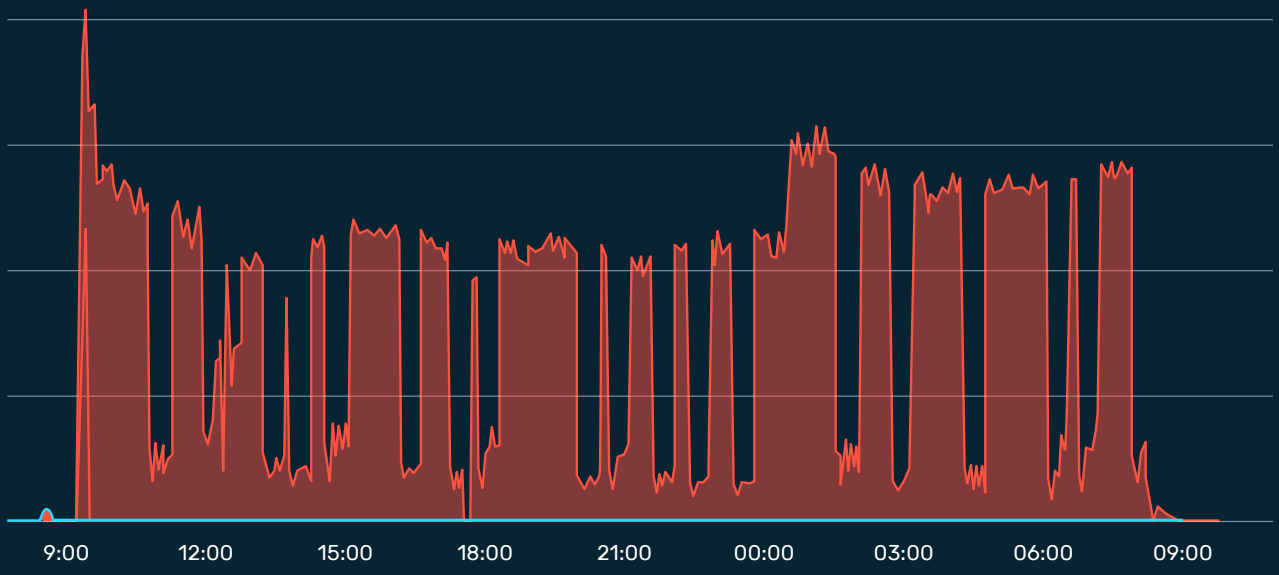
Case Study: DDoS-Angriffswelle vor den österreichischen Nationalratswahlen

Im September 2024 war über einen längeren Zeitraum hinweg eine signifikante Häufung von DDoS-Angriffen auf österreichische Organisationen im Zusammenhang mit den Nationalratswahlen zu beobachten. Am 16. September warnte das österreichische Computer Emergency Response Team (CERT.at) vor einer groß angelegten DDoS-Angriffskampagne gegen Behörden und Organisationen im Land.

Besonders betroffen waren Webseiten von Ministerien, Verwaltungsbehörden, Energieversorgern, öffentlichen Verkehrssystemen und politischen Parteien. Die Angriffe führten zu temporären Ausfällen bei mehreren wichtigen Institutionen, darunter laut Medienberichten Webseiten der Parteien ÖVP und SPÖ, des Verteidigungsministeriums, des Rechnungshofs sowie des Arbeitsmarktservices (AMS).

Eine zentrale Landesbehörde konnte dank der Schutzsysteme von Myra eine 24-stündige Attacke abwehren, sodass sie ohne Folgen blieb. Dies unterstreicht die Bedeutung robuster Schutzmaßnahmen gegen DDoS-Angriffe.

Mitigationsverlauf einer 24-stündigen Attacke



Die Grafik zeigt einen typischen DDoS-Angriff, der im Rahmen der Angriffskampagne auf österreichische Organisationen im September 2024 abgewehrt wurde. Der Angriff erfolgte in mehreren Wellen über einen Zeitraum von knapp 24 Stunden.

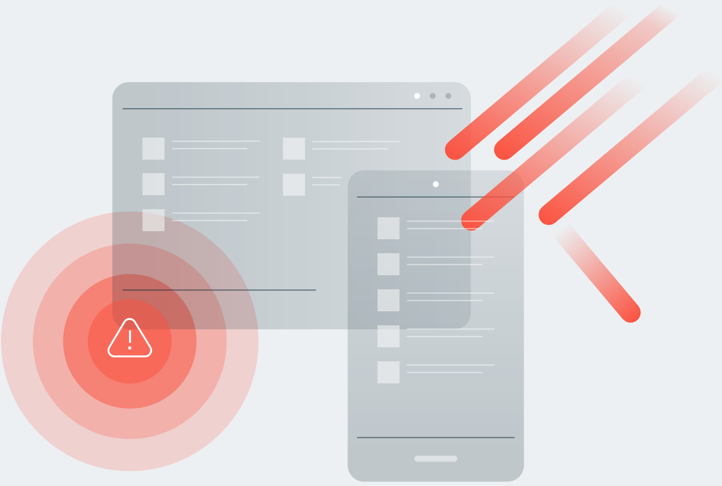
DDoS Resiliency Score macht Schutz messbar

DDoS-Schutz ist nicht gleich DDoS-Schutz. Diese Tatsache erfahren alltäglich Unternehmen weltweit, wenn ihre digitalen Geschäftsprozesse trotz vermeintlich solider Absicherung durch eine DDoS-Attacke ausgeschaltet werden.

Eine holistische Absicherung erfordert mehr als den Basisschutz, den viele Hoster und Cloud-Provider standardmäßig für die Vermittlungs- und Transportschicht (Layer 3/4) bereitstellen. Insbesondere Angriffe auf der Applikationsebene werden zunehmend komplexer und lassen sich von Schutzsystemen für Layer 3/4 nicht von validem Traffic unterscheiden.

Um Unternehmen für diese und weitere Herausforderungen bei der Abwehr von DDoS-Attacken zu sensibilisieren, wurde der DDoS Resiliency Score (DRS) ins Leben gerufen – ein Framework, das eine objektive Bewertung von Schutzmaßnahmen erlaubt und Potenziale für Verbesserungen aufzeigt.

Im Interview erläutert Markus Manzke, Chief Technology Officer (CTO) von zeroBS und DRS Board Member, wie das Framework die Schutzbereitschaft von Organisationen transparent messbar macht und welche Vorteile sich dadurch für die Optimierung der Verteidigung ergeben.



Markus Manzke,
Chief Technology Officer (CTO) von zeroBS und DRS Board Member

Was genau ist der DDoS Resiliency Score (DRS)?

Der DRS ist ein Standard zur objektiven und quantitativen Messung und Bewertung von Strategien zur Abwehr von DDoS-Angriffen. Er bietet eine standardisierte Skala, um die Stärke und Komplexität von Angriffen sowie die Fähigkeit, diesen standzuhalten, zu quantifizieren. Anhand des DRS können Unternehmen die Widerstandsfähigkeit ihrer Systeme gegenüber DDoS-Risiken bewerten.

Warum ist ein solcher Score notwendig?

Trotz der Fülle an verfügbaren Daten und Lösungen gibt es bisher keine standardisierte Skala zur Bewertung von DDoS-Abwehrmaßnahmen. Der DRS füllt diese Lücke und ermöglicht es Organisationen, ihre Bereitschaft gegen verschiedene Arten und Ausmaße von DDoS-Angriffen granular einzuschätzen.

Wie können Organisationen den DRS konkret nutzen?

Zum einen dient der DRS zur objektiven und strukturellen Bewertung ihrer Schutzbereitschaft gegen DDoS-Angriffe. Diese Bewertung ermöglicht eine bessere Evaluierung verfügbarer Schutzmaßnahmen und vereinfacht die Kommunikation von technischen Teams hin zum Management. Daraus ergeben sich datenbasierte Entscheidungsprozesse.

Zum anderen können B2B-IT-Unternehmen wie Schutzanbieter, Scrubbing-Zentren, Internetdienstanbieter (ISPs), Cloud Provider oder auch Hoster den DRS nutzen, um regulatorische Vorgaben (DORA, TIBER, NIS-2) hinsichtlich Servicequalität oder IT-Risikomanagement zu erfüllen.

Welche Faktoren behandelt der DRS?

Der DRS basiert auf sieben aufsteigenden Stufen von DDoS-Angriffen. Jede Stufe bringt zusätzliche Angriffsarten, raffiniertere Angriffsvektoren und ein größeres Traffic-Volumen mit sich. Entsprechend steigen die Anforderungen an die Verteidigung, wobei jede Stufe eine kürzere Reaktionszeit zur Schadensbegrenzung und eine geringere Latenz erfordert.

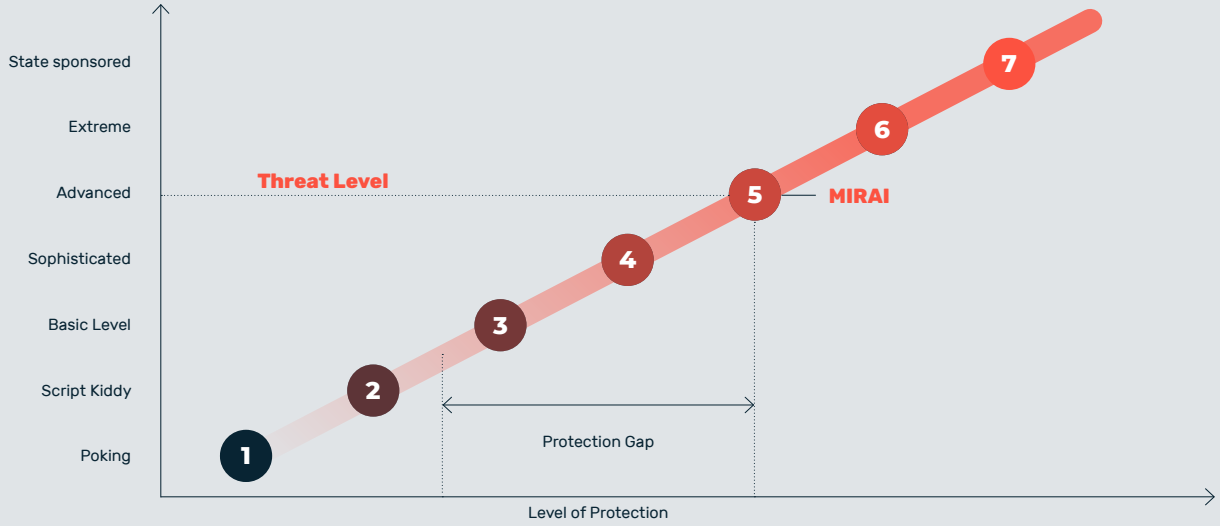
Für wen ist der DRS konzipiert?

Der DRS kann von verschiedenen Gruppen eingesetzt werden: Sicherheitsberater können den Standard nutzen, um besseren Service für Endkunden zu bieten; Anbieter von DDoS-Stresstests können den DRS verwenden, um objektive und vergleichbare Tests durchzuführen; Schutzanbieter können den DRS in ihren Entwicklungszyklus integrieren, um SLAs und Compliance-Anforderungen zu erfüllen.

Welche weiteren Vorteile bietet die Verwendung des DRS für Schutzanbieter?

Durch die Anwendung des DRS können Anbieter den Aufwand für das Incident Management reduzieren, Ausfallzeiten minimieren und den Personalbedarf optimieren. Dies führt zu Kosteneinsparungen, verringert Risiken im Zusammenhang mit der Servicebereitstellung sowie SLA-Verletzungen und verschafft einen Wettbewerbsvorteil.

DDoS Resiliency Score (DRS) auf einen Blick



Stufe	Bezeichnung	Volumen	Anfragen pro Sekunde (RPS)	Anzahl Angriffsvektoren
1	Poking	100 MBit	1.000	1
2	Script Kiddy	1 GBit	5.000	2
3	Basic Level	100 GBit	10.000	5
4	Sophisticated	500 GBit	100.000	10
5	Advanced	1.000 GBit	1 Mio	Unbegrenzt
6	Extreme	Unbegrenzt	Unbegrenzt	Unbegrenzt
7	State sponsored	Unbegrenzt	Unbegrenzt	Unbegrenzt

Der DRS verfolgt einen quantitativen Ansatz zur Messung der DDoS-Resilienz. Mit jeder Stufe von 1 bis 7 steigen die Anforderungen an das Abwehrvolumen, die Anzahl der Anfragen und die verwendeten Angriffsvektoren. In den beiden oberen Leveln für Extreme und State Professionals sind zunehmend komplexe Angriffsmethoden und das Sophistication Level entscheidend.

Automatisierung trifft Präzision: Über die Herausforderungen effizienter Cyberabwehr

Christof Klaus
Director Global Network Defense
bei Myra Security

Die zunehmende Professionalisierung von Cyberkriminellen und der Einsatz moderner Technologien wie künstlicher Intelligenz für schädliche Zwecke erfordert eine Adaption der Verteidigungsstrategie – effiziente Abwehrmaßnahmen sind jetzt gefragt.

Die Lösung von Myra: Hochautomatisierte Systeme erfassen, verarbeiten und analysieren den globalen Datenverkehr im Myra DNS in Echtzeit, um Anomalien in Sekundenbruchteilen zu identifizieren und entsprechende Abwehrmaßnahmen einzuleiten. Dieser Ansatz ermöglicht eine wesentliche Steigerung der Abwehreffizienz trotz steigender Komplexität der Angriffe.

Im Interview berichtet Christof Klaus, Director Global Network Defense bei Myra Security, worauf es bei einer schnellen und effektiven Cyberabwehr ankommt und welche Rolle KI aufseiten von Angreifern und Verteidigern spielt.

Welche Technologien setzt Myra ein, um Angriffe schnell und effizient abzuwehren?

Zur Erkennung und Abwehr von Angriffen setzen wir eine Vielzahl unterschiedlicher Mechanismen ein. Erkenntnisse über Angriffe und Zugriffsmuster werden immer an den dafür geeignetsten Stellen gewonnen. Entweder wird dann bereits an dieser Stelle eine Gegenmaßnahme eingeleitet, oder die hier generierten Daten werden mit an anderer Stelle ermittelten Erkenntnissen zusammengeführt und dann in einem größeren Kontext ausgewertet.

Was sind die Herausforderungen bei der Entwicklung eines hochautomatisierten Schutzsystems?

Auch die Herausforderungen bei der Entwicklung dieser Systeme sind vielfältig. Einigen davon kann durch gut geplante Investitionen in Hardware begegnet werden. Hier geht es direkt um Aspekte wie Rechenleistung, Bandbreiten, Geschwindigkeiten, Schnittstellen und dergleichen. Andere Herausforderungen, insbesondere im Analytics-Umfeld, können wiederum nur durch sehr gezielt entwickelte Softwarelösungen gelöst werden. Hier sind neben den reinen Leistungsanforderungen an solche Lösungen auch architektonische Aspekte wie horizontale Skalierbarkeit, Redundanz, aber auch Flexibilität und gezielte Anpassbarkeit von höchster Bedeutung.

> *„Fakt ist, dass man sich heutzutage holistisch vor allen Angriffsarten schützen muss, denn ein unmitigierter Angriff – egal auf welcher Ebene – hat immer negative Auswirkungen auf das Gesamtsystem."*

Wie hilft die Myra-Technologie dabei, auch unbekannte und komplexe Angriffsmuster frühzeitig zu erkennen und abzuwehren?

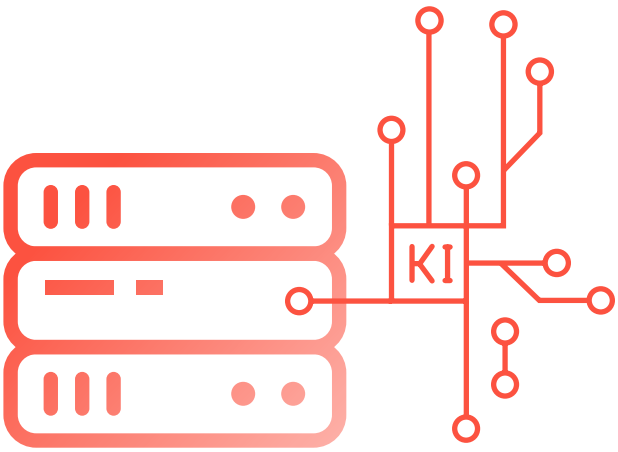
Bei der Abwehr von Angriffen sind zwei Aspekte besonders wichtig. An erster Stelle steht die Notwendigkeit, den eigentlichen Angriff zu erkennen. Zumeist gibt es in diesen Fällen sehr deutliche Veränderungen zum „Normalbetrieb", sei es ein starker Anstieg des Traffics oder beispielsweise eine Häufung von WAF-Triggern. Die zweite, deutlich komplexere Anforderung besteht dann darin, den „guten" von „bösem" Traffic zu unterscheiden und diesen selektiv herauszufiltern. Hier ist Myra mit seiner Technologie sicherlich einen Schritt voraus. Ein weiterer Aspekt, der es uns ermöglicht, besonders effektiv und schnell vorzugehen, ist, dass das Ausspielen von sehr spezifischen – auf den jeweiligen Angriff exakt zugeschnittenen – Blockregeln innerhalb von Sekundenbruchteilen im gesamten CDN erfolgt.

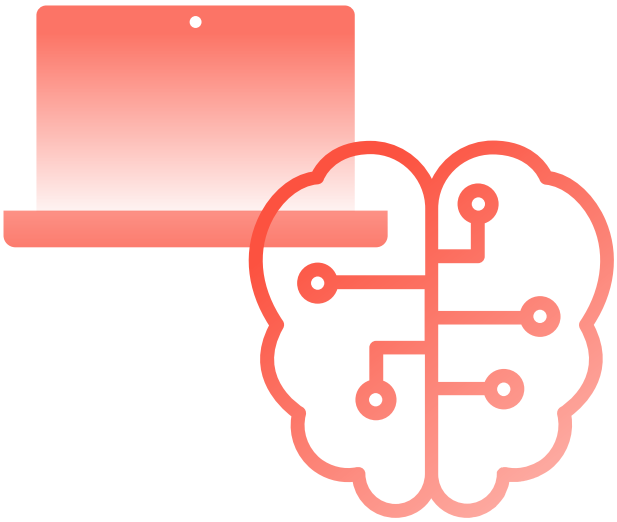
Wie unterscheidet sich die automatisierte Abwehr im Bereich des Netzwerk- und Infrastrukturschutzes vom Anwendungsschutz?

Der sicherlich deutlichste Unterschied zwischen Infrastruktur- und Applikationsschutz ist die Menge an Daten, die zur selektiven Abwehr eines Angriffs zur Verfügung steht. Beim Applikationsschutz kann aus den jeweiligen Anwendungsprotokollen und -parametern detailliert entnommen werden, was bei einem Aufruf passiert und wie das Besucherverhalten zu interpretieren ist. Der Traffic auf Infrastrukturebene ist nicht entschlüsselt und bietet somit eine deutlich geringere Informationsmenge zur Regelbildung. Eine GET-Flood oder ein Cachebuster-Angriff auf HTTPS sieht auf der unentschlüsselten Netzwerkebene eben nur nach sehr viel Traffic auf Port 443 aus und kann somit nur schwer von validem Datentraffic unterschieden werden. Hier muss man dann auf andere Parameter wie IP-Reputation, GeoIP-Datenbanken und weitere Analysemittel zurückgreifen, um den schädlichen Traffic abzuwehren. Fakt ist, dass man sich heutzutage holistisch vor allen Angriffsarten schützen muss, denn ein unmitigierter Angriff – egal auf welcher Ebene – hat immer negative Auswirkungen auf das Gesamtsystem.

Blick auf die Gegenseite: Welche Herausforderungen entstehen durch den zunehmenden Missbrauch von KI als Angriffstool?

KI-gestützte Systeme bieten insbesondere einen Geschwindigkeitsvorteil gegenüber menschlichen Akteuren. Einer KI stehen innerhalb kürzester Zeit nach Veröffentlichung einer Schwachstelle diese Informationen zur Verfügung und sie kann diese anwenden. Weiterhin ist es möglich, diese neuen Attacken praktisch vollautomatisiert mit Techniken wie WAF-Evasion und anderen Angriffsvektoren zu kombinieren, bis ein erfolgreiches Resultat erzielt wird. Dies erhöht den Druck auf die Dienstanbieter immens, veröffentlichte Schwachstellen innerhalb kürzester Zeit zu beheben und solide Abwehrsysteme in Stellung zu bringen, um weiterhin sicher zu sein.





Wie nutzen Angreifer KI konkret für Attacken, abseits von Phishing?

Ein weiterer Vorteil von KI ist neben dem bereits angesprochenen Zeitfaktor, die Fähigkeit, Angriffsmuster noch während des Angriffs zu modifizieren. Insbesondere im Bereich des Applikationsschutzes beobachten wir Versuche, die Identifikation des Angreifers zu erschweren, indem ganze Parametergruppen zufällig während eines Angriffs verändert werden. Dies erhöht die notwendige Sophistication der Mitigationssysteme erheblich, um immer noch effektiv verteidigen zu können.

Welche Grenzen haben Automatisierung und KI in der Cybersicherheit und wo bleibt menschliches Eingreifen notwendig?

KI-Systeme können extrem schnell und effizient vorgehen. Oft aber eben auch nur in genau den Bereichen, in denen sie trainiert wurden. Neue Anwendungsfelder sind ihnen nur schwer zugänglich oder nur im Rahmen „allgemeiner" Anpassungen. Wann immer also ein Gesamtüberblick, das Verständnis des Zusammenspiels einzelner Services, tiefes Expertenwissen oder aber einfach der Umgang mit zuvor unbekannten Situationen erforderlich ist, bleibt der Mensch in seiner Adaptionsfähigkeit unübertroffen. Dies gilt sowohl für Angreifer als auch für Verteidiger.

Quellen und Referenzen

1 BKA: Organisierte Kriminalität - Bundeslagebild 2023
2 Bitkom Wirtschaftsschutz 2024
3 https://www.gdv.de/gdv/medien/medieninformationen/mehr-cyberschaeden-praevention-wichtiger-denn-je-181946
4 Bitkom Wirtschaftsschutz 2024
5 Capgemini Research Institute 2024: New defenses, new threats: What AI and Gen AI bring to cybersecurity
6 ISC2 Cybersecurity Workforce Study 2024
7 Bitkom Wirtschaftsschutz 2024
8 ENISA Threat Landscape Report 2024
9 https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem
10 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-shuts-down-27-ddos-booters-ahead-of-annual-christmas-attacks
11 Bitkom Wirtschaftsschutz 2024
12 ENISA Threat Landscape Report 2024
13 ENISA Threat Landscape for DoS Attacks November 2023
14 https://www.dw.com/de/gro%C3%9Fe-cyberattacke-trifft-ministerien-in-frankreich/a-68499200
15 https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/kfu.html
16 https://www.vrt.be/vrtnws/de/2024/10/07/websites-belgischer-behoerden-im-visier-eines-cyberangriffs-eine/
17 ENISA Threat Landscape Report 2024
18 https://www.bleepingcomputer.com/news/security/romanias-election-systems-targeted-in-over-85-000-cyberattacks/
19 https://www.spiegel.de/ausland/rumaenien-praesidentschaftswahl-muss-wiederholt-werden-a-5040d09f-e6ae-4ca4-8a60-122a9c7b4ce0
20 https://www.krone.at/3580528
21 https://www.tagesschau.de/inland/verfassungsschutz-warnung-cyberangriffe-bundestagswahl-100.html
22 ENISA Compendium on Elections Cybersecurity and Resilience 2024
23 European Union External Action - 2nd EEAS Report on Foreign Information Manipulation and Interference Threats
24 https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfakes-demean-defraud-disinform/

Deshalb entscheiden sich CISOs für Myra

Security

Durch Cyberangriffe werden Daten gestohlen, Systemausfälle provoziert und Kommunikationskanäle gestört. Myra wehrt Angriffe auf Ihre digitalen Prozesse in Echtzeit ab.

Performance

Traffic-Peaks durch Sales- Kampagnen, Livestreaming oder unplanbare Ereignisse überfordern Web-Anwendungen. Myra liefert Ihren Content immer hochperformant aus.

Business Continuity

Myra gewährleistet den größtmöglichen Schutz für Ihr Unternehmen, indem es direkte und georedundante Verbindungen zu Ihrer Infrastruktur nutzt, ohne von externen Faktoren abhängig zu sein.

Compliance

Gesetzliche und unternehmensspezifische Vorgaben zu IT-Sicherheit und Datenschutz erfordern auditierte Prozesse. Myra ist Ihr Garant für strengste Anforderungen.

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.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0667-2024 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 Testat Typ 2 | Trusted Cloud | IDW PS 951 ISAE 3402 | KRITIS Nachweis gemäß § 8a. Abs. 3 BSIG | ISO 9001:2015

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 (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | KRITIS-Betreiber gemäß § 8a Abs. 3 BSIG | Qualitätsmanagement nach ISO 9001

Myra schützt, was zählt. In der digitalen Welt.

1&1 versatel | Bundeszentrale für gesundheitliche Aufklärung | llb 1861 | msc Munich Security Conference | CANCOM | DSV IT Service | Barmenia Einfach. Menschlich. | flatex DEGIRO

Made in Germany

Myra schützt, was zählt.
In der digitalen Welt.

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.

Cyberangriffe sind teuer,
ein unverbindliches Gespräch kostet nichts.

Myra Security GmbH

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