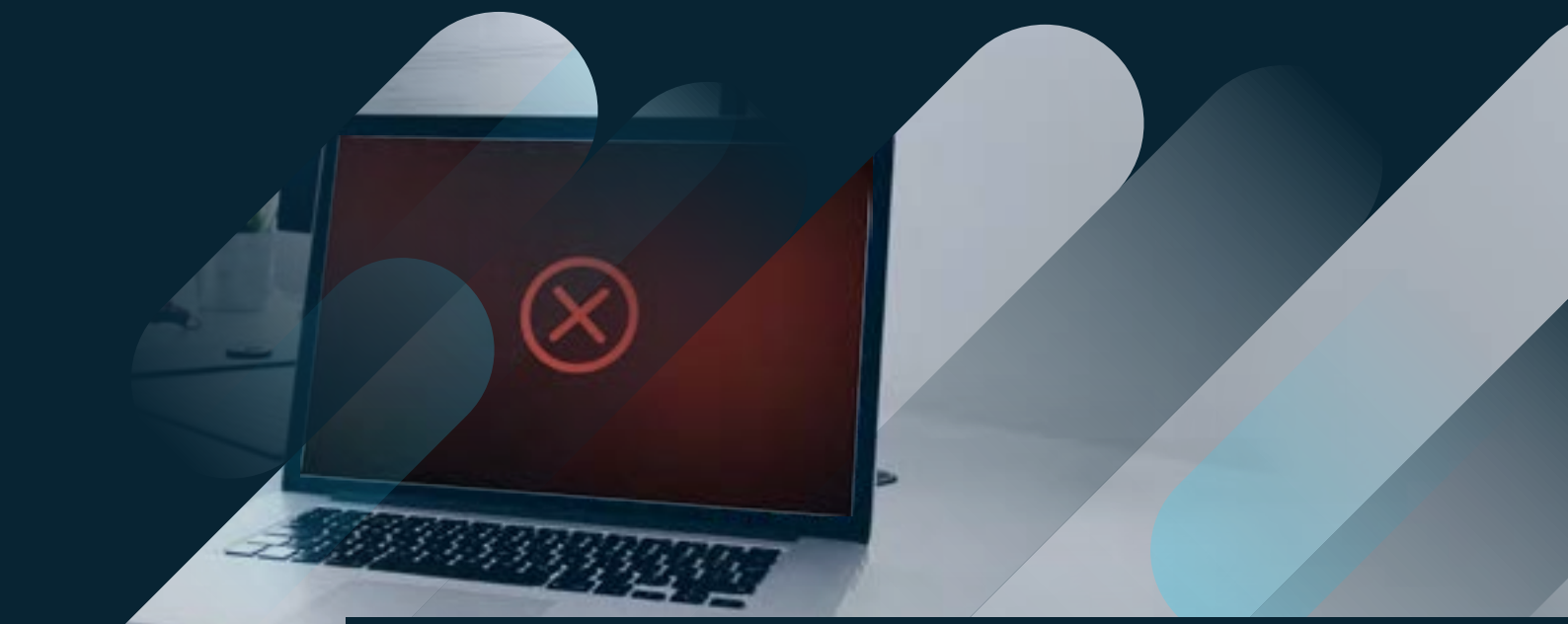


MYRA

FACT SHEET

Die 9 wichtigsten Downtime-Ursachen und wie Sie sie vermeiden

Die 9 wichtigsten Downtime-Ursachen und wie Sie sie vermeiden

Verfügbarkeit, Performance und Ausfallsicherheit zählen zu den wichtigsten Kriterien beim Hosting von Webseiten, Internetportalen und APIs. Fallen Onlinedienste aus und bleiben für längere Zeit nicht erreichbar, bedeutet das für die betroffenen Organisationen meist hohe Schäden. Je nach Business-Kritikalität des ausgefallenen Webprozesses, Branche und Unternehmensgröße variieren die minütlichen Kosten für Downtime von niedrigen dreistelligen Beträgen bis hin zu Summen im mittleren sechsstelligen Bereich.

Der Ausfall von Webressourcen kann vielerlei Ursachen haben. Das Spektrum reicht von Konfigurationsfehlern von Software über externe Angriffe durch Cyberkriminelle bis hin zu Hardware-Defekten oder geplanten Wartungsarbeiten.

Nachfolgend erhalten IT-Entscheidungsträger einen schnellen Überblick über die verbreitetsten Ursachen von Downtime und über geeignete Maßnahmen zur Downtime-Reduzierung.

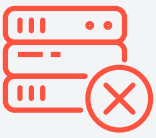
Primäre Ursachen für Ausfallzeit

DNS-Fehler/-Attacken

Überlastung

DDoS-Attacken

Sicherheitsprobleme



Hardwarefehler

Softwareprobleme

Provider-/Hoster-Probleme

Wartung

Stromausfälle

DNS-Fehler/-Attacken:

Fehler bei der Konfiguration der DNS-Namensauflösung oder Ausfälle des verwendeten DNS-Dienstanbieters können dazu führen, dass Onlinedienste nicht mehr für Nutzer zugänglich sind. In der Vergangenheit haben Ausfälle großer Anbieter wie Dyn zu weitreichenden Downtimes im Internet geführt und eine Reihe der Traffic-stärksten Webseiten im Netz lahmgelegt.

Tipp: DNS-Server stellen lukrative Ziele für Cyberkriminelle dar. Angreifer können mit gezielten DDoS-Attacken auf Nameserver die darüber verwalteten Onlineprozesse unzugänglich machen. Ferner lassen sich DNS-Server auch als Waffe missbrauchen, etwa für DNS-Amplification-Angriffe oder für DNS-Spoofing, um Anfragen auf andere Webseiten umzuleiten. Aus diesem Grund sollten DNS-Server über dedizierte Schutzsysteme vor Angriffen von außen abgesichert sein und die Implementierung von DNSSEC-Erweiterungen unterstützten, um die Integrität von Servern und Verbindungen zu validieren. Alternativ kann auch die gesamte Namensauflösung an Dienstleister mit der erforderlichen IT-Sicherheitskompetenz übertragen werden.

9/10 (88%) Unternehmen waren von DNS-Attacken betroffen

IDC-Studie aus 2022

Überlastung:

Wenn der Server zu viele Anfragen gleichzeitig bearbeiten muss, kann dies dazu führen, dass er überlastet wird und nicht mehr reagiert.

Tipp: Wenn Performance-Probleme gehäuft auftreten, ist das ein Anzeichen für unzureichende Hardware-Ressourcen. Über stärkere und/oder zusätzliche Webserverinstanzen lassen sich solche Probleme beseitigen. Alternativ sorgen CDN-Services für die benötigte Performance durch eine Spiegelung der Inhalte auf global verteilten Servernetzen – ohne Aufwände für zusätzliche Hardware. CDN-Services bieten zudem die erforderliche Flexibilität, um kurzzeitige Traffic-Spitzen infolge von Marketing-Kampagnen, Livestreams oder Shopping-Events bedarfsgerecht auszugleichen.

13,65 TBit/s

Traffic-Rekord am DE-CIX – 13.09.2022

DE-CIX

DDoS-Attacken:

Cyberkriminelle nutzen Botnetze und andere Angriffsmethoden, um Webseiten mit Anfragen zu überfluten und zu überlasten. Webressourcen ohne dedizierte Schutzsysteme gehen bei solchen Angriffen zwangsläufig in die Knie. In den vergangenen Jahren hat sich die DDoS-Bedrohungslage massiv verschärft. Die Mitigationszahlen aus dem Security Operations Center (SOC) von Myra belegen für das erste Quartal 2023 einen Zuwachs schädlicher Serveranfragen um 220 Prozent im Vergleich zum Vorjahr.

Tipp: Dedizierte Schutzlösungen auf Netzwerk- und Applikationsebene sichern die Verfügbarkeit von Webressourcen auf allen relevanten Layern ab. Insbesondere die Verteidigung von Layer-7-Angriffen bereitet vielen Unternehmen immer noch Probleme. Die Wahl eines geeigneten Schutzdienstleisters mit der erforderlichen Branchenerfahrung ist daher der Schlüssel für eine erfolgreiche Absicherung kritischer Onlineprozesse.

+220%

schädliche Requests in Q1 2023

Myra Security

Sicherheitsprobleme:

Cyberkriminelle infiltrieren und übernehmen Server-Instanzen mittels Brute-Force-Angriffen wie Credential Stuffing oder Credential Cracking. Auch neu entdeckte Sicherheitslücken (Zero-Day-Exploits) oder noch nicht geschlossene Schwachstellen dienen Angreifern als Einfallstor. Solche Attacken können für Unternehmen in Serverausfällen, unkontrolliertem Datenabfluss und, je nach Art der betroffenen Daten, in Datenschutzverstößen und Bußgeldern resultieren.

Tipp: Eine Web Application Firewall (WAF) in Kombination mit Bot Management erlaubt eine umfängliche Absicherung von Webservern, um die gängigsten Angriffsvektoren zu adressieren, die etwa in den OWASP Top 10 enthalten sind. WAF-Lösungen erlauben sogar, kurzfristig auf neue Sicherheitsprobleme zu reagieren, für die es noch keine Software-Aktualisierungen gibt.

Hardwarefehler:

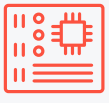
Hardwareprobleme wie Festplattenfehler, defekte Netzteile oder Überhitzung können dazu führen, dass Server ausfallen – ob nun im eigenen Rechenzentrum oder beim Hoster. Eine ITIC-Umfrage ergab, dass die meisten technischen Ausfälle vor allem auf ausgefallene Festplatten zurückgehen (58%), gefolgt von defekten Hauptplatinen (43%) und fehlerhaften Prozessoren (38%).

Tipp: Redundant aufgebaute Serverstrukturen sind weniger anfällig für Hardwarefehler, da im Notfall die Last von anderen Serverinstanzen übernommen wird. Kommt zusätzlich eine CDN-Lösung zum Einsatz, können durch Stale-Objects Inhalte sogar bei einem Ausfall aller Origin-Server weiterhin an die Besucher und Besucherinnen der Webseite ausgespielt werden.

Ursachen technischer Ausfälle durch defekte Bauteile

58%

Festplatten



43%

Hauptplatinen

38%

Prozessoren

ITIC-Umfrage

Softwareprobleme:

Bugs oder Konfigurationsfehler in BIOS, Betriebssystem, Hypervisor, Treiber oder Anwendungen können dazu führen, dass Webserver abstürzen oder nicht mehr reagieren. Zu den verbreitetsten Problemen zählen veraltete Betriebssysteme sowie fehlerhaft aufgespielte Patches und Upgrades der Server-Software. Insbesondere bei hoher Belastung quittieren schlecht aufgesetzte Systeme ihren Dienst.

Tipp: Grundsätzlich sollten Betriebssysteme für Server über eine Minimalinstallation aufgebaut sein, die sich auf die absolut benötigten Komponenten beschränkt. Auf diese Weise lässt sich die virtuelle Angriffsfläche auf ein Mindestmaß reduzieren. Ebenso sollten Aktualisierungen geschäftskritischer Software nicht automatisch erfolgen. Vielmehr müssen Patches ausgiebig in einer Testumgebung (Sandbox) auf Herz und Nieren geprüft werden, um Fehler in Produktivsystemen auszuschließen. Die Einbindung von Software in ein Patch-Management sichert die Aktualität der eingesetzten Komponenten und hilft dabei, Schwachstellen schnellstmöglich zu beheben.

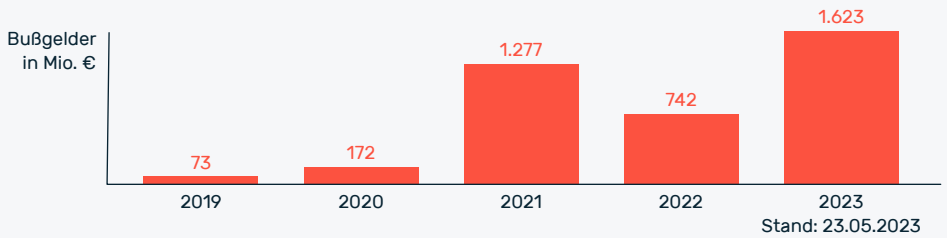
Provider-/Hoster-Probleme:

Wenn Webserver extern über Hoster betrieben oder CDN- und Security-Dienste als Cloud-Lösung eingesetzt werden, besteht immer eine Abhängigkeit zum jeweiligen Anbieter. Dieser ist dafür verantwortlich, alle erforderlichen und vorgeschriebenen Maßnahmen umzusetzen, um Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der ausgelagerten Dienste sicherzustellen. Darüber hinaus gilt es, alle regulatorischen Vorgaben zu beachten, um Datenschutzverstöße zu vermeiden und andere Compliance-Herausforderungen zu meistern.

Tipp: Bei der Wahl des geeigneten Providers/Hosters spielt neben technisch-prozessualen Vorgaben an Performance, Sicherheit und Nachhaltigkeit auch die erforderliche Compliance eine zentrale Rolle. Insbesondere personenbezogene Daten dürfen entsprechend der Datenschutz-Grundverordnung (DSGVO) ausschließlich im Europäischen Wirtschaftsraum (EWR) sowie in sicheren Drittländern übertragen und verarbeitet werden. An Anbieter mit Sitz in unsicheren Drittländern wie den USA dürfen personenbezogene Daten nur durch den Einsatz von zusätzlichen Sicherheitsmaßnahmen wie Verschlüsselung und/oder Pseudonymisierung übertragen werden. Dies dient der Absicherung des Datenschutzniveaus bei der Verarbeitung oder Weiterleitung sensibler Informationen. Technisch bedingt sind solche Maßnahmen für einige Einsatzszenarien jedoch ungeeignet, wie etwa bei Diensten für CDN, Web Application Security oder DDoS-Schutz. Diese Services erfordern im Gegenteil eine Offenlegung verschlüsselter Inhalte (SSL/TLS-Terminierung), um schädlichen Traffic gezielt zu filtern.

Darüber hinaus sollten Firmen darauf achten, Dienstleister mit sogenannter Bad Neighborhood zu vermeiden. Darunter versteht man Anbieter, die auch Kunden aus Branchen wie der Erwachsenenunterhaltung, Glücksspiel oder Gaming unter Vertrag haben, die tendenziell stärker von Angriffen und Sabotageversuchen betroffen sind. Die verschärfte Bedrohungslage dieser Branchen birgt das Potenzial, dass Angriffe auf diese Ziele auch die Sicherheit und Performance für andere Kunden negativ beeinflussen.

Compliance-Stolperstein DSGVO: Bußgelder erreichen neues Rekordhoch



enforcementtracker.com, European Data Protection Board

Wartung:

Geplante Wartungsarbeiten können dazu führen, dass der Server vorübergehend offline ist. Eine routinemäßige Wartung von Webservern ist grundsätzlich empfehlenswert, um Ausfällen vorzubeugen. Solche Wartungsarbeiten umfassen in der Regel eine Reinigung der Hardware zur Überprüfung der Luftströme, das Testen der Festplatten auf Speicherintegrität, das Testen und Aufspielen von Patches und Updates sowie das Auslesen und Prüfen der anfallenden Logdateien.

Tipp: Durch den Einsatz virtualisierter Server können Workloads umverteilt werden, um eine Downtime zu umgehen. Darüber hinaus lassen sich Wartungsfenster auch über CDN-Lösungen mittels Stale-Objects überbrücken, bis die Origin-Server wieder verfügbar sind.

Stromausfälle:

Stromausfälle oder Stromschwankungen können dazu führen, dass Server ausfallen oder beschädigt werden.

Tipp: Geschäftskritische Prozesse sind mit georedundanten Serverstrukturen vor lokalen Ereignissen wie Stromausfällen oder Naturkatastrophen geschützt. Über Dienstleister mit global verteilten Servernetzen lässt sich die Verfügbarkeit von Diensten ebenfalls absichern, indem die erforderlichen Inhalte auf einem CDN gespiegelt werden.

12,7 Minuten

sind Verbraucher pro Jahr im Schnitt ohne Strom (Haushalte, Gewerbe, Industrie)

Bundesnetzagentur

Mit Know-how, Redundanz und starken Partnern zum Uptime-Champion

Ungeplante Ausfallzeiten sind unvermeidbar. Jedoch können Sie als Entscheidungsträger die dringendsten Ursachen von Downtime wirksam angehen und somit die bestmögliche Verfügbarkeit und Sicherheit Ihrer Webprozesse gewährleisten. Damit verschaffen Sie sich einen Wettbewerbsvorteil.

Die meisten Maßnahmen zur Minimierung von Downtime können inhouse durch Ihre IT umgesetzt werden. Je größer jedoch die Skalierbarkeit und der Schutzbedarf sind, desto wirtschaftlicher ist eine Kooperation mit externen Partnern, die sich auf Sicherheits- und Performance-Dienstleistungen spezialisiert haben.

Auf technischer Ebene sollten Sie auf die Umsetzung etablierter Best Practices setzen, die dafür erforderlichen Lösungen implementieren und strategische Partnerschaften mit starken Unternehmen eingehen. Dadurch stellen Sie sicher, dass Ihre Webressourcen hochverfügbar sind.

→ **Machen Sie die entscheidenden Schritte hin zum Uptime-Champion und lassen Sie Ausfallzeiten der Vergangenheit angehören. Kontaktieren Sie uns noch heute für eine individuelle Ersteinschätzung:** +49 89 414141 - 345 oder info@myrasecurity.com

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

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