Digital Value Creation under Threat: Blackout Risk from DDoS Cybercrimes?

The information superhighway as a bottleneck: When denial-of-service attacks bring data traffic to a standstill, it threatens to disrupt the highly networked business models of today. Now is the time for businesses to reckon with this rapidly growing risk and take action.

Digitalization is the true success story of our era. And yet as technological innovations become more powerful and new business models triumph, companies become increasingly vulnerable to attack. Cloud computing, IoT, AI and real-time applications are innovations that generate massive data streams, increase complexity and create a growing number of attack vectors for wide-ranging cybercrimes.

Even worse, the potential damage they can cause is growing as well. After all, in just the past few years, the number of critical building blocks in today's value chains that use digital tools has soared. The 2021 AXA Future Risks Report ranks cyber risk second among the top risks worldwide. According to Germany's Federal Office for Information Security (BSI): "Successful digitalization demands cybersecurity."

The office used its most recent security report to warn the public about digital threats. In addition to ransomware attacks, which have been widely discussed in the media, distributed denial-of-service attacks (DDoS) in particular are causing serious damage.

MAKING AN IMPACT THAT MATTERS since 1845

In these attacks, malicious actors disrupt the normal traffic of servers and other IT resources by overwhelming them with a flood of requests until they crash and bring data exchange to a standstill. One of the most prominent cases of this type in recent years was the DDoS attack on the New Zealand stock exchange in August 2020, which halted trading for several days. BSI recently highlighted just how serious the threats have become: The alert level for DDoS attacks was raised specifically around Black Friday 2021, and in fact there was a 200 percent increase in DDoS activity on Black Friday and Cyber Monday compared with the previous year.

However, there is still a lack of awareness surrounding DDoS attacks that lags behind the growing number of these cybercrimes. This Point of View takes a closer look at the risk posed by DDoS attacks and highlights possible methods of defense. After all, we cannot take concrete steps toward building sustainable cyber resilience until we identify the nature and the scale of the threat. The cyber risk facing the German economy is not an unknown quantity. According to a study by a digital industry association, cybercrimes caused a whopping 220 billion euros in damage during 2020/21, more than double the losses incurred in 2018/19. It is clear that companies need to urgently step up their efforts in this area.

Threat situation: DDoS attacks as a leading global risk

Cybercriminals have a wide range of different attack methods in their arsenal, and they are becoming more technologically sophisticated every day. At 27 percent, DDoS attacks are the second most damaging cyberattacks in the ranking published by Bitkom – just behind to ransomware attacks at 31 percent. Fast approaching the top risk spot today, DDoS attacks were ranked only 6th in 2018/19. The security experts at Link11 show further evidence for the growing risk in their latest DDoS report. For example, there was a 33 percent increase in the number of DDoS attacks in the first half of 2021 alone.

> "DDoS attacks are the second most damaging cyber risks, and they are growing at a disturbing and record-breaking rate."
>
> **Marc Wilczek, Chief Operating Officer Link11**

More detailed metrics confirm this trend, as seen in the increase in maximum attack volume by 36 percent and in maximum packet rate by 147 percent. Compared to the first quarter of 2021, the number of seriously dangerous high-volume attacks rose by 19 percent in the second quarter alone.

What kind of real-world implications do these numbers have for the businesses involved and their stakeholders? Attacks often lead to severe disruptions that paralyze large portions of a company's day-to-day operations – with potentially catastrophic consequences in sectors like healthcare or infrastructure. The DDoS report from Link11 outlines some particularly high-profile attacks from the first half of 2021. In January, for example, DDoS attacks on German school platforms disrupted pandemic-related distance learning. In the UK, the US, Germany and other countries, bad actors launched attacks on the booking websites for COVID-19 vaccinations. The France-based AXA Group changed the terms of their cyber insurance policies last May, which prompted a wave of DDoS and ransomware attacks on the group's offices in Asia. Several web hosting providers in Ireland experienced outages lasting several hours after widespread attacks on internet service providers. And a DDoS attack on a provider's data centers caused major disruption to the online banking services of Germany's cooperative banks.

The motives of the perpetrators launching these DDoS attacks are varied. For some, criminal extortion (monetary demands) is the goal, particularly as the risk of detection is relatively low – an attractive proposition for members of an organized crime syndicate. By establishing a criminal business model based on a division of labor, they can make their attacks more effective and more efficient. In other cases, there are political motives ("hacktivists"). Geopolitical links and government intelligence occasionally play a role as well, using advanced technology that is in some instances only available to state actors. More often than not, however, we must assume that sabotage is the only motive, a pure desire for destruction or personal revenge.

Taking vulnerability to a new level

The increase in cyberattacks in general and in DDoS attacks in particular are mainly attributable to the increased vulnerability of today's companies, and there are numerous drivers at play. Today's highly integrated global value chains mean that cyberattacks impact companies not only directly, but also indirectly, for example as customers of the service providers involved. As digitalization advances, IT problems no longer only affect a limited portion of the business, say, for instance, the company website, but potentially the entire company as a whole.

This can have dangerous knock-on effects in which the failure of a single component brings the entire organization to its knees and causes a total blackout. Or a domino effect in which a single incident triggers a potentially catastrophic chain reaction.

Companies today are increasingly forced to face risks that are outside their own sphere of influence. One reason for this is the way services and capabilities are shifting away from on-site installations to the cloud. In this context, UK insurer Lloyds of London calculated some time ago that the failure of a single large cloud provider for three to six days could cost the economy as much as 15 billion dollars in the US alone. The indirect vulnerability also extends to other fields, e.g., when a payment service provider crashes. Industrial manufacturers and other traditional "hardware" companies are feeling the impact as well. Under the banner of Industry 4.0, information technology and operational technology are becoming increasingly intertwined, and more and more of these companies are transforming into "as a service" providers. Vulnerability increases even more when you introduce innovations such as the Internet of Things (IoT), which extend beyond corporate boundaries thanks to supply chain connectivity and ecosystem partner integration.

> "The challenge for companies today is to mitigate risks that have potentially serious consequences but are increasingly beyond their control."
>
> **Ralph Noll, Partner Cyber Risk Deloitte Germany**

What is more, a lot of today's applications rely on real-time data, which by definition makes them more vulnerable.

Even private individuals are feeling more vulnerable to cybercrime, particularly since the pandemic and the boom in remote working. Networked e-health apps and devices are particularly exposed, as they may impact a person's health. There are also a serious data protection risk in this context as well.

In the area of consumer products, connected cars, smart devices (fitness trackers, etc.) and smart household appliances may also be vulnerable to attack. The risk here goes beyond the unfortunate failure of a household appliance to the potential of manipulative hijacking, perhaps without the consumer's knowledge. Your smart device could become part of a botnet of willing, remote-controlled "zombie armies" that can be mobilized for extortionate DDoS attacks. The most recent Meris attack, for example, relied on a botnet of 250,000 devices worldwide. Last but not least, bad actors are now even targeting the public sector, where government institutions have digitalized public services for citizens and businesses alike.

As companies grapple with these vulnerabilities, which promise to get worse over time, it is more urgent than ever to become aware of the associated risks – not only in terms of the immediate financial and operational harm, but also with regard to reputational damage and liability risk beyond the standard warranties. There are also significant regulatory risks in relation to new regulations or those currently in the pipeline, such as GDPR, the EU AI Act (artificial intelligence) or the EU Digital Operational Resilience Act (DORA), which carry heavy penalties for certain violations.

Attacks are becoming more complex and more sophisticated

Advances in digital technology are of course accessible to criminal actors as well, and they play a key role in the recent rise in DDoS attacks. Attack methods are becoming more efficient and more effective thanks to the massive opportunity offered by digitalization, including on the part of the attackers. The entire endeavor is obviously becoming professionalized, all the way to the reality of "cybercrime-as-a-service". This enables bad actors without technological expertise to take advantage of "DDoS as a service" and launch attacks with minimal effort.

The attacks are also becoming more complex in several respects. The number of multi-vector DDoS attacks, which simultaneously target technical vulnerabilities in transport, applications and protocols (e.g., UDP, TCP), is growing exponentially. They accounted for 65 percent of all cyberattacks in the first half of 2021, while single-vector attacks decreased from 48 percent to 35 percent year-on-year. As every vector demands its own defense strategy, the more vectors there are, the more difficult it becomes to find an effective defense. We have even seen attacks with upwards of twelve vectors. 45 percent of the incidents involved two vectors, while 42 percent involved three vectors.

Another complex DDoS threat involves so-called reflection amplification attacks. These are indirect multi-vector attacks that exploit certain types of servers and services that are not configured to protect against them. They initially receive malicious data packets in a limited volume, which in many cases are then forwarded to the actual target in an amplified form. This type of attack most frequently targets DNS services (42%), followed by DVR DHCPDiscovery at 29 percent. The malicious actors in this segment are also becoming more innovative over time. A relatively new form of attack involves Session Traversal Utilities for NAT (STUN), targeting the STUN servers that enable communication with VoIP devices (e.g., telephones) behind the firewall.

DDoS attacks can become exponentially more effective when they operate bots in the cloud as opposed to standard bots. 35 percent of all DDoS attacks rely on this method, using the vulnerabilities of cloud providers to compromise server instances and turn them into bots. This makes the attack much more effective due to the large amount of traffic on the cloud.

This increases the potential attack volume by a factor of one thousand, and the customers affected often do not notice the misuse until much later. However, bad actors may actually rent cloud capacity themselves, using stolen credit card data for example. Cloud DDoS attacks most often target AWS services (Amazon, 27%), followed by Google Cloud (15%) and Microsoft Azure (11%). As the boom in cloud computing continues, we can expect this type of attack to increase as well.

"We are seeing more and more cybercriminals use a combination of attack methods – ransomware, DDoS and publishing stolen corporate information on the dark web – ramping up the pressure to pay their ransom demands."

Ralph Noll, Partner Cyber Risk Deloitte Germany

The gaps in existing defenses

DDoS attacks are not really all that new. Despite the fact that bad actors started staging overload attacks against servers in the early days of the internet, this type of cybercrime is anything but obsolete.

The increase in complexity we described above makes DDoS protection more relevant than ever. However, given the recent rise in this threat, our conventional security measures fall seriously short. A lot of companies rely on the standard DDoS protection offered by their telecom service providers, which are typically quite weak. After all, DDoS defense is not among a carrier's core competencies, and the protection they offer often fails to cover all of the necessary layers, is not properly configurable and lacks the capacity to defend against more serious attacks. The carriers themselves are often overwhelmed when an attack occurs, opting for a null-routing response in many cases, e.g., simply discarding the relevant data traffic for days on end – not exactly a satisfactory solution for the client. Another factor here is the cost of data transmission, which can quickly turn defense against such an attack into a loss proposition. All the more reason for companies to take a closer look at a carrier's SLAs and fee conditions before they sign. This type of protection also runs the risk of becoming indirectly vulnerable in a DDoS attack that targets the provider itself.

In principle, mounting a defense via local hardware is also an option, but it requires serious effort. The indiscriminate "blanket bombing" of modern DDoS attacks with a volume upwards of 1 Tbps could bury a company's conventional 10Gb connection many times over; even 100-gig connections would be hopelessly overwhelmed. To say nothing of the special team of experts a company would have to keep on hand 24/7. Even the frequently used method known as Generic Route Encapsulation Tunneling (GRE Tunneling) often has weaknesses and limitations, particularly when huge data volumes are involved.

It lacks sufficient error correction capabilities, suffers from unstable latency and is prone to loss. Low throughput rates and the overhead cost of tunneling are additional drawbacks. Given the rapidly growing threat and the weakness of existing protection mechanisms, it is time to find a new model to defend against DDoS attacks

Some cloud-based services from specialist providers offer clients the ability to stand on equal footing with cloud-based attackers and mount an effective defense.

New methods for a new threat level

Today's DDoS risk is reaching new heights both qualitatively and quantitatively. And companies not only have to launch a defense that keeps up with this trend – they also need to stay one step ahead of it for the foreseeable future. That will require moving away from obsolete security paradigms to state-of-the-art cyber defenses instead, e.g., zero trust, automation and a risk-oriented strategy. Zero trust involves a fundamental reversal in the burden of proof. Essentially, the system does not trust any process or actor without an in-depth analysis, regardless of whether it comes from inside or outside certain corporate parameters. Forward-looking DDoS security strategies automate all of these processes, as is the case with Link11's specialized algorithms. They rely on sophisticated technologies such as artificial intelligence (AI) and machine learning (ML). Gone are the days of classic pattern recognition, the focus is now on automated real-time analyses of anomalies in data traffic (e.g., sources and packets). This approach makes the defense methods much faster and more precise. Cloud-based resource reserves from dedicated data centers allow for real-time rectification, replacing the time-consuming patch/fix approach of the past. These methods are also scalable to defend against even high-volume attacks. The cloud-based approach ensures the necessary redundancy, which is an important factor in protecting against server failure in an overload situation.

Geo-redundancy is guaranteed thanks to the global distribution of traffic, with the added bonus of the favorable price point and effective cost control that come with cloud-based deployment.

The efficient use of resources has decisive qualitative advantages as well: Thanks to this smart approach, a risk-oriented overall strategy helps companies allocate resources properly. They can set up their own individual, risk-specific data profile and ensure that sensitive information and processes are more protected internally.

The practical steps to putting a security strategy in place

Risk-oriented strategy is a key success factor as we try to become more resilient against DDoS attacks. It starts by analyzing in depth which digital assets in your company are worth protecting and which are essential for your business to remain in operation. This risk assessment should be part of a general inventory of your company's cyber maturity, creating a robust foundation for your cyber strategy. At the same time, whatever approach you choose must be aligned with your overall corporate strategy. There are also other areas within a company that need cyber-relevant initiatives, for example the physical security of a company facility. It is essential to assess these initiatives using meaningful tests in war games and other simulations to improve cyber resilience at the staff level as well. Finally, integrating new security providers into the existing process landscape, both in technical and procedural terms, is an issue worth considering when you are setting up a state-of-the-art DDoS defense. A comprehensive, cloud-based DDoS solution such as the one Link11 offers is a good place to start, and the specialists at Deloitte are ready to provide expert support with the implementation.

Deloitte can also help you integrate these individual initiatives into a comprehensive solution, thanks to our long-standing expertise in related cyber disciplines. When it comes to cyber resilience, Deloitte is leading the way with tried-and-tested offerings in all of the key disciplines – cyber strategy, cloud computing, data & privacy, identity, emerging technologies, application security and detect & response methods. And with the deep expertise of over 250 specialists on our team, our in-depth experience in virtually every industry as well as the international orientation of our global network, you can rest assured you have found the right partner. We will make sure your holistic cyber strategy succeeds – an essential precondition for the effective defense against

"In the 'Cyber Everywhere' era, we need cyber security in the cloud as well, providing a truly scalable solution to protect our digital assets against increasingly aggressive attacks."

Ralph Noll, Partner Cyber Risk Deloitte Germany

Sources

AXA: AXA Future Risks Report 2021
https://www.axa.com/en/press/publications/future-risks-report-2021

Bitkom: Angriffsziel deutsche Wirtschaft
https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Bitkom: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie (Studienbericht 2018)
https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI): DDoS-Entwicklungen vor Black Friday und Cyber Monday
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-269757-1032.pdf?__blob=publicationFile&v=3

CyberTalk: 250,000 strong DDoS botnet, "record shattering" attacks
https://www.cybertalk.org/2021/09/13/250000-strong-ddos-botnet-record-shattering-attacks/

Deloitte: Cyber Security Report 2021
https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html

Deloitte: The Future of digital identity
https://www2.deloitte.com/global/en/pages/risk/articles/the-future-of-digital-identity.html

Deloitte: The trust enabler. Building cyber-security strategies for a trusted, digital future
https://www2.deloitte.com/us/en/insights/topics/digital-transformation/digital-trust-for-future.html

Deloitte Future of Cyber Risk 2035: Vier Zukunftsszenarien
https://www2.deloitte.com/de/de/pages/risk/articles/future-of-cyber-risk-2035.html

Deloitte: Zero Trust. Paradigmenwechsel in der Cybersecurity
https://www2.deloitte.com/de/de/pages/risk/articles/zero-trust.html

Link11: Distributed Denial of Service Report für das 1. Halbjahr 2021
https://www.link11.com/de/downloads/ddos-report-h1-2021

Link11: Record Number of Cyber Attacks over Black Friday
https://www.link11.com/en/blog/threat-landscape/record-number-of-cyber-attacks-over-black-friday-weekend/

Lloyd's: Failure of a top cloud service provider could cost US economy $15 billion
https://www.lloyds.com/about-lloyds/media-centre/press-releases/failure-of-a-top-cloud-service-provider-could-cost-us-economy-15-billion-dollars

Contact

Ralph Noll
Partner | Risk Advisory
Tel: +49 211 8772 2285
rnoll@deloitte.de

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's more than 345,000 people worldwide make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Issue 04/2022