LINK11

WHITEPAPER

UK: Critical infrastructures in the crosshairs

In cooperation with:

PENNINGTONS MANCHES COOPER

Content

Threat to critical infrastructure from sabotage and cyber-attacks grows

Hundreds of cyber-attacks are reported yearly to the UK's cyber security regulators. As technological advances and digitisation increase the prevalence of systems and processes that are undertaken online, the threat to such systems from global cyber criminals increases in tandem.

In a recent wave of cyber-attacks, the Russian hacker group NoName has set its sights on multiple UK government institutions and organisations, causing significant disruptions with DDoS attacks[1]. These attacks are believed to be part of a larger, ongoing campaign aimed at European organisations, with the hackers specifically targeting entities with a pro-Ukraine stance. As these assaults continue, the affected institutions and the cybersecurity community at large are on high alert, working to mitigate and counteract the growing threat.

Distributed Denial of Service (DDoS) attacks are increasing – such attacks aim to overwhelm a target's network or website with a flood of traffic or requests, rendering it inaccessible or significantly reducing its performance. During the Covid-19 pandemic, DDoS attacks increased worldwide as cybercriminals sought to exploit the digital vulnerability of businesses and remote working populations. In doing so, most attackers followed financial motives.

Taking just another example from 2022, the Log4j – essentially a way for developers to keep track of what happens in their software applications or online services – was made public in the VMware Horizon product[2]. Within days, cyber criminals exploited this vulnerability targeting NHS Digital (the UK's national healthcare system).

More recently, on 30 June 2023, the ALPHV or BlackCat ransomware group listed Barts NHS Trust on its website as a victim of a cyber-attack perpetrated by the group[3]. They claim to have exfiltrated 7TB of data, which is said to include personally identifiable data. If true, this would be one of the biggest cyber-attacks in the UK to date. However, as is the nature of ransomware attacks, this may be a false claim designed to extort the NHS Trust. These examples highlight the scale, diversity and potential consequences of major cyber-attacks in the UK.

Cyber-attack threats have also increased for critical infrastructure (CRITIS) operators. On the one hand, there have been rapid technological advances in recent years; on the other, there has been a significant increase in the number of decentralised, networked systems. This has increased the potential target pool for cyber-attacks. According to the World Economic Forum experts, a real "cyber storm" is brewing. The current "Global Cybersecurity Outlook"[4] also shows that 91% of the executives surveyed expect far-reaching and catastrophic cyber incidents in the coming years. The UK government estimated that cyber-attacks cost the UK economy around GBP 27 billion every year[5], with 39% of UK businesses reporting suffering a cyber-attack in 2022 (a figure which is no doubt understated, given the reluctance to publish details of cyber-attacks). In addition, the companies surveyed expect a further increase in cyber-attacks.

The number of politically motivated DDoS attacks also increased significantly in 2022 following the invasion of Ukraine. The goal of such attacks is to weaken the population's morale and cause the greatest possible damage, as Microsoft stated in the report "Defending Ukraine: Early Lessons from the Cyber War"[6].

"The mutability of DDoS attacks is enormous. This makes it all the more important to analyse traffic in real-time using smart, fast and secure methods."

Jurij Zykov, Account Executive, Link11

On 15 May 2023, the pro-Russian hacker group "Killnet" declared cyber war on several countries, including the United States, Great Britain, Germany, Italy, Latvia, Romania, Lithuania, Estonia, Poland and Ukraine. The consequences of this declaration have already been felt in Germany, Italy, Lithuania, Norway, and Poland. Hardly a month went by without a cyber-attack on NATO countries, their public institutions, banks, or CRITIS.

The DDoS attacks defended against in the Link11 network in 2022 were, on average, slightly fewer in number and shorter in duration but more intense and demanding to defend. An analysis of the attacks registered in the Link11 network shows that the critical load for DDoS attacks in 2022 was reached on average just 55 seconds after the attack began. In comparison, attacks in 2021 took an average of 184 seconds to reach their peak.

These "turbo attacks" can cripple the network even before defences take effect. Moreover, these attacks and the methods used are constantly changing. Instead of randomly attacking businesses in the hope of success, highly targeted, advanced and sophisticated DDoS attacks are now being used.

Important processes are too rarely rehearsed so that in an emergency, detecting a DDoS attack and pivoting the data line takes far too long. In such a case, precious time is lost, and business interruption ensues. In many cases, delivery models and operating concepts are no longer up to date.

Service Level Agreements (SLAs) are important in this context. Because not only is the number of DDoS attacks increasing, but their DNA is also increasingly changing. The complexity of the attacks has increased continuously in recent years. That is why advanced SLAs focus on ‘time to mitigate’ (TTM) instead of detection.

Therefore, to address this evolving threat landscape, it is crucial for legal framework conditions to ensure a certain standard of cyber security for Critical Infrastructure (CRITIS). Similarly, companies should regularly review their conditions to dispel misconceptions and avoid deluding themselves into a false sense of security.

Potential target of attacks: CRITIS

CRITIS are facilities and systems that are essential for the functioning of society and the economy, namely the critical assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them.

They include energy, food, finance and insurance, health, information technology and telecommunications, media and culture, municipal waste management, government and administration, transport and traffic, and water.

Corporations, small and medium-sized enterprises, as well as public administration and civil society, are all vulnerable to cyber-attacks, but CRITIS is at particular risk.

This is because the reliability and security of CRITIS are essential to everyday activities, so any disruption or failure has serious consequences for society.

If cybercriminals gain access to CRITIS systems, they may steal data, extort money, or even cause physical damage.

These systems are particularly vulnerable to cyber-attacks for several reasons

CRITIS are highly dependent on information technology (IT) to function effectively. This means that a successful cyber-attack on the IT systems behind CRITIS can impact their ability to function or completely paralyse them.

CRITIS are often very complex systems consisting of many different components and subsystems. This increases the number of vulnerabilities that an attacker could exploit.

Many CRITIS are or contain obsolete systems-built years or even decades ago. Such systems may use outdated or insecure technologies that are particularly vulnerable to attack.

CRITIS are vulnerable to human error since people operate and manage them. Simple human error or negligence can lead to security risks and make it easier for an attacker to gain access to the system.

In the UK, there are 13 national CRITIS sectors:

Chemicals

Chemical facilities and processors

Civil Nuclear

Nuclear power plants and waste centres

Communications

Cell towers and telephone exchanges

Defence

Military bases

Emergency services

Hospitals, prisons, and police stations

Energy

Power stations, power lines and backup generators

Finance

Banks

Food

Key production factories

Government

Government buildings (Downing Street and The Cabinet Office)

Health

Laboratories and testing facilities

Space

Launch facilities and satellites in orbit

Transport

Roads, bridges, and railways

Water

Water stations and treatment facilities

However, not everything within the national infrastructure sector is considered 'critical'. The UK Government defines Critical National Infrastructure as:

"Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a. Major detrimental impact on the availability, integrity or delivery of essential services - including those services whose integrity, if compromised, could result in significant loss of life or casualties - taking into account significant economic or social impacts; and/or

b. Significant impact on national security, national defence, or the functioning of the state."

The National Cyber Security Centre **(NCSC)** is an organisation within the UK Government responsible for protecting the Critical National Infrastructure IT networks, data and systems from cyber-attacks. The NCSC works in partnership with the National Protection Security Authority **(NPSA)**. The NPSA is the UK Government's National Technical Authority for physical and personnel protective security. It works alongside partners in government, police, industry and academia to reduce the vulnerability of the national infrastructure and increase the UK's resilience to national security threats.

Legal foundations ensure the security of CRITIS

The security of CRITIS is ensured by a well-developed and constantly evolving legal and regulatory framework. Various statutory and regulatory provisions include measures to ensure uniform security across the network and information systems of CRITIS.

Overview of the legal basis

The UK General Data Protection Regulation **(UK GDPR)**

Whilst the UK GDPR does not set out explicit cyber-security requirements, it does impose obligations on the processing of personal data by businesses, including the providers of CRITIS. This includes the following:

- Data controllers have an obligation to minimise the amount of personal data processed, and they should only process data that is necessary for their purposes.
- Data controllers should only collect data where necessary and delete it as soon as it is no longer required.
- Data controllers must have technical and organisational measures in place to demonstrate that they comply with data protection principles.
- In some circumstances, data controllers and processors must designate a data protection officer who is the main point of contact with the Information Commissioner's Office **(ICO)**.
- Data controllers and processors should not transfer personal data outside of the UK unless there is a lawful basis to do so.
- Data controllers should consider data protection at the design stage of any processing operation, which should, for example, include ensuring sufficient technical and organisational measures are in place to ensure that the personal data is secure.

The UK GDPR sets out a "security principle" that requires personal data to be processed to ensure the "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The UK GDPR further prescribes that data controllers and processors must implement technical measures (e.g., firewalls, antivirus software and threat-detection) and organisational measures (e.g., policies and procedures) to ensure a level of security appropriate to the level of risk.

When a security event leads to a personal data breach, data processors must notify the controller without delay. A data controller must notify the ICO within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Network and Information Systems Regulations 2018 (SI 2018/506) **(NIS Regulations)** transpose the requirements of the Network and Information Security Directive (EU) 016/1148 (**Cybersecurity Directive)** into UK law. They impose various cybersecurity and incident reporting obligations. The NIS Regulations focus on the security of IT systems, rather than the personal data processed by those systems. They also impose cybersecurity and incident reporting obligations on Operators of Essential Services **(OESs)** and Relevant Digital Service Providers **(RDSPs)**.

OESs

OESs are operators of an essential service in the key sectors of energy, transport, health, drinking water supply and distribution, and digital infrastructure, where that operator relies on network and information systems and satisfies the threshold requirements for the type of essential service they provide. Under the NIS Regulations, OESs have two main obligations. They must take appropriate and proportionate:

1. Technical, organisational measures to manage risks posed to the security of the network on which their essential service relies. Given the state of the art, these measures must ensure a level of security for network and information systems that is proportionate to the risk.

2. Measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used to provide an essential service to ensure the continuity of those services.

When carrying out the above duties, the OESs must consider any relevant guidance issued by its designated competent authority.

An OES must notify its competent authority without undue delay and no later than 72 hours after becoming aware of any incident that has a significant impact on the continuity of the essential service the OES provides, having regard to:

- the number of users affected by the disruption.
- the duration of the incident.
- the geographical area affected by the incident.

RDSPs

An RDSP, on the other hand, is a provider that satisfies certain criteria. An RDSP must:

1. Provide the following types of digital service in the UK:
    - an online marketplace
    - an online search engine
    - a cloud computing service

2. Employ more than 50 people.

3. Have an annual turnover or balance sheet total exceeding EUR 10 million (that is, not a micro or small enterprise (as defined in Commission Recommendation 2003/361/EC).

4. Either have a head office in the UK or a nominated representative established in the UK.

RDSPs must identify and manage (through appropriate and proportionate measures) the risks posed to the security of the network and information systems on which they rely to provide, within the UK, either an online marketplace, online search engine or cloud computing service.

These measures must:

- Ensure a level of security of network and information systems appropriate to the risk posed, having regard to the state of the art.

- Prevent and minimise the impact of incidents affecting their network and information systems to ensure the continuity of those services; and

- Consider the following elements as specified in Article 2 of Regulation (EU) 2018/151:
    - the security of systems and facilities
    - incident handling
    - business continuity management
    - monitoring, auditing and testing
    - compliance with international standards

In addition, RDSPs must notify the ICO without undue delay and in any event no later than 72 hours after becoming aware of any incident having a substantial impact on the provision of any of the digital services mentioned above, providing sufficient information to enable the ICO to determine the significance of any cross-border impact.

The UK Government has proposed changes to the **NIS Regulations** following its post-implementation review. These changes include:

- Expanding the "digital services" scope to include "managed services". Managed services are defined by meeting the following characteristics:
  - services supplied to a client by an external supplier.
  - regular and ongoing service management.
  - categorised as business-to-business services.
  - reliant on network and information systems.
- Applying a new, two-tier supervisory regime for all RDSPs.
- Creating new delegated powers to enable the government to update the framework and scope of the NIS Regulations without an Act of Parliament.
- Creating a new power to bring organisations within the remit of the NIS Regulations where that organisation is critically dependant on entities already in the scope of the NIS Regulations.
- Strengthening existing incident reporting duties to include significant incidents beyond those that impact service.
- Extending the existing cost recovery provisions to allow regulators (such as Ofcom, Ofgem, and the ICO) to recover the entirety of reasonable implementation costs from the companies that they regulate.

The Cybersecurity Directive is being repealed and replaced at the EU level by the Directive (EU) 2022/2555 (**NIS 2 Directive**) from 18 October 2024. The UK will not implement this as it is no longer bound by EU legislation. However, the NIS 2 Directive has an extraterritorial reach; it applies to non-European Economic Area "digital service providers" who offer services in the European Economic Area.

"The threat of a cyber attack is very real and ever-increasing, in part due to the further adoption of technology as well as an increased sophistication of attackers. All sectors should be concerned, but the critical infrastructure sector is at particular risk because of the devasting effects a cyber attack could have on society at large. For this reason, critical infrastructure organisations need to go above and beyond to ensure systems and processes are secure and protected."

Charlotte Hill, Partner, Penningtons Manches Cooper LLP

More uniformity through the Cyber Assessment Framework

In December 2022, the UK Government published the National Cyber Strategy 2022[7], which states the UK Government's vision: that "the UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests". To achieve this, the UK Government will lead the way by adopting the Cyber Assessment Framework (CAF) as the assurance framework for the government.

The NCSC developed the CAF to support operators of essential services under the NIS Regulations, as well as more widely across the private sector, including CRITIS sectors. It provides a framework for assessing compliance against the following principles: managing security risk, protecting against cyber-attacks, detecting cybersecurity events, and minimising the impact of cybersecurity incidents. Each principle is supported by a collection of relevant guidance, which highlights some of the factors that an organisation may need to consider when deciding how to achieve the outcome and recommends ways to tackle common completion challenges. Organisations subject to the NIS Regulations should continue to follow the guidance set by their competent authority. However, organisations affected by the NIS Regulations will likely find the CAF guidance useful.

Regulatory authorities and enforcement

Numerous regulators enforce cybersecurity-related laws and regulations in the UK, which CRITIS organisations will be subject to.

The UK GDPR is enforced by the ICO, which has the power to act against both controllers and processors in breach of the UK GDPR. The ICO has four main enforcement powers:

1. Information notices: the ICO can request a controller, processor or individual to provide it with certain information within a specified time frame.

2. Assessment notices: the ICO can issue a notice indicating that it intends to investigate compliance with data protection legislation through, for example, inspection, examination or interview of a relevant individual.

3. Enforcement notices: the ICO can require a controller or processor to perform a specific action to comply with information rights and/or to remedy a breach.

4. Penalty notices: the ICO can issue a notice levying a sanction on a controller or processor.

Under the UK GDPR, the ICO has the power to enforce fines of up to GBP 17.5 million or 4% of annual worldwide turnover, whichever is higher.

Notably, in 2020, the ICO issued a monetary penalty notice fining Marriot International around GBP 18.4 million for processing personal data without adequate security measures, leaving about 339 million guest records exposed to a cyber-attack. The same year, the ICO also fined British Airways GBP 20 million for processing personal data without adequate security measures, leaving 400,000 customers vulnerable to a cyber-attack. More recently, in October 2022, CRITIS organisation, Interserve, was fined GBP 4.4 million for failing to put in place adequate security measures to prevent a cyber-attack.

OESs are not regulated by a single, unified body. Instead, regulation is sector specific – OESs are regulated by various designated competent authorities. These are set out in Column 3 of the table in Schedule 1 of the NIS Regulations[8].

In contrast, RDSPs are regulated by a single, unified body – the ICO. It takes on this regulatory function in addition to enforcing the UK GDPR (as set out above).

Organisations in breach of the NIS Regulations may be subject to a maximum fine of GBP 17 million for a material contravention that the enforcement authority determines has caused or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the UK economy. The NIS Regulations also give competent authorities powers to serve information notices, conduct inspections to assess an organisation's systems and serve enforcement notices setting out the steps an organisation must take to rectify an issue.

"It is vital that critical infrastructure providers understand their legal and regulatory requirements, in order to avoid the possible sanctions imposed following a breach."

Tom Perkins, Associate, Penningtons Manches Cooper LLP

Risk avoidance is not only for CRITIS

Overall, the regulatory and legal landscape explored above is designed to achieve the highest level of security possible. All CRITIS organisations and companies must comply with the UK GDPR, whilst OESs and RDSPs are required to comply with the NIS Regulations and guidance issued by the relevant competent authority. Breaches of the relevant law or regulation pose a risk to the public and can result in enforcement action and potentially significant monetary sanctions. It is, therefore, essential for CRITIS organisations to continually consider their cyber security obligations.

As explained above, CRITIS organisations are popular targets for cyber-attacks. Therefore, these organisations must meet the minimum cyber security thresholds required by law and regulation. The reality of human error should also not be underestimated. CRITIS organisations must proactively raise their standards and manage risk to protect against all possible risks.

In addition, they should continually review the adequacy of existing cybersecurity coverage and consider implementing more stringent measures to ensure maximum security. It is advisable that CRITIS organisations do this annually. This will help ensure that CRITIS organisations adhere to their legal and regulatory obligations and avoid exposure to enforcement action and/or unwieldy fines while maintaining the CRITIS organisations' focus on such obligations.

It is important that some specifications and standards increase cyber protection. However, implementing standards can only be one part of comprehensive cybersecurity management. All operators of CRITIS must also take proactive measures to protect their systems and data from cyber-attacks.

Deep Dive Banking: Comprehensive regulation ensures higher cyber protection

Some areas within CRITIS already fulfil a high level of cyber protection due to regulatory requirements or specific industry standards, such as the financial sector. In the UK, financial services providers such as banks, insurance companies, credit unions and financial advisers are regulated by either the **Financial Conduct Authority** (FCA) and the **Prudential Regulatory Authority** (PRA) jointly or by the FCA only. They are subject to additional security and governance obligations directly or indirectly related to cybersecurity.

The FCA Handbook[9] and PRA Rulebook[10] contain provisions that regulate the financial services industry. In general terms, the specific FCA and PRA requirements that apply depending on the type of financial services provider, the nature of the financial services being provided and the nature of the relevant customers. The PRA views cyber-attacks considering its financial stability objective, whilst the FCA views them considering its consumer protection and market integrity objectives.

The FCA Handbook includes Principles for Businesses. The following principles relate to cyber-resilience:

- Principle 3 of the Principles for Businesses – a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

- Principle 11 of the Principles for Businesses – a firm must deal with its regulators openly and cooperatively. It must appropriately disclose to the appropriate regulator anything relating to the firm of which that regulator would reasonably expect notice.

Principle 11 is further considered in the context of a cyber event on the FCA's website, which states that a firm must report a cyber-attack that:

- results in significant loss of data.
- results in the availability or control of its IT systems.
- impacts many victims. Or
- results in unauthorised access to its information and communication systems.

Principle 11 is further expanded upon in Rule 15.3.1R of the Supervision Manual[12] in the FCA Handbook, which states that if an incident could have a "significant adverse effect on the firm's reputation; or ... could affect the firm's ability to continue to provide adequate services to its customers", then a notification must be made immediately.

The FCA Handbook also includes a Senior Management Arrangements, Systems and Controls (**SYSC**) part and the following points relate to cyber-resilience:

- SYSC 3.1.1 – a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business.
- SYSC 3.2.6 – a firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime.

The **PRA** has eight 'Fundamental Rules' like the FCA's Principles for Businesses. Of particular interest is:

- Fundamental Rule 2: a firm must conduct its business with due skill, care, and diligence
- Fundamental Rule 5: a firm must have effective risk strategies and risk management systems
- Fundamental Rule 6: a firm must organise and control its affairs responsibly
- Fundamental Rule 7: a firm must deal with its regulators openly and cooperatively. It must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice

In the cyber-resilience context, the Fundamental Rules are supplemented by the Risk Control part of the PRA Rulebook. The rules in this part of the PRA Rulebook cover risk control, risk committee and group arrangements. They are derived from the Capital Requirements Directive IV and the Markets in Financial Instruments Directive II.

The FCA and the PRA are responsible for enforcing breaches of the regulations applicable to financial services industries, including the requirements in the FCA Handbook and the PRA Rulebook. Notable fines imposed include:

- GBP 3 million was issued by the FSA (the FCA's predecessor) against three HSBC firms for various data security failings, including, in two separate incidents, unencrypted data on a disk and a CD being lost in the post.
- GBP 1.26 million was issued by the FSA against Norwich Union Life for failing to implement effective systems and controls to protect customer data, which led to some customers suffering fraud.
- Approximately GBP 2.3 million was issued by the FSA against Zurich Insurance plc after a subcontractor, which was not adequately supervised, lost an unencrypted backup tape with data relating to 46,000 customers.
- Approximately GBP 16.4 million was issued by the FCA against Tesco Personal Finance plc in connection with a cyber-attack, including for failure to take appropriate action to prevent the foreseeable risk of the cyber-attack and failure to respond with sufficient rigour, skill and urgency.
- GBP 56 million was issued by the FCA and the PRA against the RBS Group for inadequate testing procedures and failure to establish robust IT systems, which gave rise to consumer disruption as over 6.5 million customers could not access their accounts online for several weeks.

Catching up with CRITIS: Who still needs to do the most?

In contrast to the highly regulated financial sector, several CRITIS still have some catching up to do regarding their cyber security. Here are some examples:

1. **Energy supply** is central to the functioning of society and the economy. However, the increasing interconnection of power grids and smart grid technologies creates new attack targets for cybercriminals. A successful cyber-attack on the energy supply can lead to significant disruptions in the power grid and, in the worst case, to a nationwide blackout. IBM's Security Report[12] last year identified the energy sector as the primary target of cyber-attacks in 2021, with 24% of all UK cyberattacks targeted at the sector.

2. **Transport networks** and, in the future, autonomous vehicles are likely targets for cybercriminals as hackers can manipulate them to cause traffic chaos and even accidents. In addition, airports and train stations are vulnerable to cyber-attacks as they increasingly rely on digital systems to control air and train movements. In September 2022, for example, bus operator "Go-Ahead" suffered disruption to its services (accounting for 11% of the UK's buses and Transport for London bus routes) due to a cyber-attack[13].

3. **Healthcare:** Hospitals, doctors' offices and other medical facilities store sensitive patient data that hackers can steal. A cyberattack on the healthcare sector can also lead to medical equipment and systems being tampered with, which can put patients' health at risk. In 2022, the NHS 111 non-emergency telephone, used by thousands of patients daily for healthcare advice over the phone, was forced offline after a major ransomware attack[14].

A closer look at the area of energy supply reveals the great need to catch up in various places. One important aspect is the supply chain. Many energy suppliers purchase important components and services from third parties such as software and hardware providers, engineering service providers or subcontractors. This can lead to vulnerabilities in the supply chain being exploited to penetrate their systems and expose CRITIS to major risk.

Another factor is the increasing digitalisation and networking of energy supply systems, especially in connection with the introduction of smart grid technologies. Outdated IT systems and insufficient cyber awareness among employees also play a major role in CRITIS vulnerabilities.

Overall, there is a need for a clear definition of CRITIS and a continuous improvement of their cyber security measures with a close look at the supply chains. This is the only way to ensure they are sufficiently protected against potential cyber-attacks.

"The reality of human error should not be overlooked. Critical infrastructure operators must be proactive in taking steps to mitigate human mistakes in cyber security through effective training and comprehensive policies and guidance."

Oliver Kidd, Partner, Penningtons Manches Cooper LLP

Meaningful IT security strategy required

It is undisputed that digitalisation and networking are also advancing within CRITIS. In the future, the use of artificial intelligence will increase, and more and more automated systems will communicate digitally with each other. This makes producers and suppliers in the energy sector, banks in the financial sector or hospitals in the healthcare sector – the name just a few - more vulnerable to attack. Cyber-attacks result in production downtimes worth millions and supply bottlenecks, which, in the final analysis, can even endanger human lives or, in the worst case, even cost them.

On 19 April 2023, the NCSC warned of DDoS attacks[15] (along with website defacements and the spread of misinformation) against Western CRITIS by state-aligned adversaries supporting the Russian invasion of Ukraine. National CRITIS organisations are vulnerable because of their role in providing essential public services.

The many examples in the Link11 DDoS Report 2022 show the impact DDoS attacks can have on CRITIS companies and organisations. These include, for example, the attacks on political institutions in Norway, Germany and other NATO countries, the attack on the Port of London and the failure of the Austrian Federal Railways ticketing system.

The question is, therefore, are they sufficiently protected?

Against the backdrop of the ever-increasing number of cyber-attacks, operators of CRITIS and companies must deal with the topic of digital threats and the corresponding protection mechanisms.

As soon as more than a ransom is at stake, cybe-rattacks' effects target business capability and take on societal dimensions.

Companies should structure their IT systems in such a way that an attack has only minimal impact and critical parts of the network are not reached. Particularly in the CRITIS sector, an end-to-end and integrated IT security system is required regarding national security to ensure smooth operations.

Carrier-based models or the use of local hardware are no longer sufficient, as these approaches usually require the manual detection and reactive panning of data traffic. This process is often lengthy and error-prone in practice. Depending on the company's operating model, ITIL-compliant IT operations require approvals for implementing an emergency change and the manual notification of the provider. At the same time, human error occurs in many cases. In such cases, precious time is lost, and business interruption is almost certain. Regardless of the technology used, the operational concept alone shows systemic weaknesses and is no longer up to date.

Furthermore, the carrier-based models are partly backed by minimally equipped SLAs. There is usually no guaranteed protection bandwidth or a contractually guaranteed time-to-mitigate (**TTM**) for all types of attacks. To make matters worse, the carrier reserves the right to drop all traffic for the duration of the attack. This so-called zero routing can sometimes last for hours or days, as happened with the New Zealand Stock Exchange in 2021.

Why CRITIS should protect themselves against DDoS attacks:

1. Business interruption: DDoS attacks can lead to CRITIS no longer being able to provide their services properly. This business interruption can have a negative impact on public safety and welfare.
2. Reputational damage: if CRITIS are unavailable due to DDoS attacks, this can lead to a loss of trust and have a longer-term impact.
3. Data loss and manipulation: DDoS attacks can be used as a diversionary tactic to simultaneously steal or manipulate confidential data that is essential to the functionality of the infrastructures.
4. Cybercriminal motivations: Cybercriminals or state actors can use DDoS attacks to exert political pressure on governments, sabotage CRITIS or extort ransom.

“As cybercriminals become more sophisticated, the vulnerability of critical infrastructure sectors increases exponentially. It is imperative to adopt an end-to-end, integrated IT security system that ensures smooth operations and mitigates attacks with minimal impact. The time for comprehensive protection is now, as the stakes have never been higher.”

Jurij Zykov, Account Executive, Link11

Effective IT protection solutions for the future

Link11 offers effective IT solutions that comprehensively protect companies from cyber threats and strengthen their cyber resilience. Using artificial intelligence and machine learning ensures continuous data traffic monitoring. Traffic is filtered in real-time to detect and respond to anomalies or attacks quickly. Unlike traditional solutions, Link11 provides a highly scalable, automated, and accurate defence against DDoS attacks that can stop even complex attacks.

On-premises solutions are mostly unable to stop complex attacks. For example, low-bandwidth attacks, so-called carpet-bombing attacks, often infiltrate the radar and cause the IT backend to collapse.

By the time an attack reaches a company's IT systems, it is already too late. On the other hand, cloud-based solutions can filter, analyse, and even block traffic in real-time before it gets anywhere near a company's IT systems.

Finally, the supply chain disruptions in the wake of the COVID-19 pandemic clearly demonstrated how interconnected and vulnerable our information, goods and payment flows are today. Companies must therefore take precautions to effectively mitigate the impact and duration of DDoS attacks at a technical level. At the strategic level, companies need to identify, assess, and ultimately mitigate the full breadth and depth of internal but also cross-company risks. In the area of CRITIS, this implies selecting its partners from the point of view of resilience to cyber-attacks and deploying the appropriate protection mechanisms.

Traditional protection solutions for network and infrastructure security too often rely on manual assessment of incidents and static, pattern-based assessment of data. This time- and resource-intensive approach has no future in the face of the growing complexity of IT security. New attack techniques undercut the radar because they do not fit the pattern. The existing automation does not take effect - the damage follows. The sensible and effective IT security strategies include permanent questioning and simulation of the emergency and automated solutions to minimise the weaknesses in the operating models and human error and ensure the necessary protection.
Link11 relies on artificial intelligence, machine learning, automation, and real-time defence with its integrated cloud security platform for the holistic protection of IT infrastructures and critical applications and to strengthen cyber resilience. Based on these key technologies, the Link11 Cloud Security Platform comprehensively protects businesses from cyber threats at the web and network levels.

If you want to protect your infrastructure, networks, and applications against cyber-attacks, talk to the cyber resilience experts at Link11. Link11's integrated cloud security platform offers a holistic solution based on the latest technologies to protect businesses from adaptable, complex, and intense DDoS attacks.

Penningtons Manches Cooper LLP: cyber security and cybercrime legal services

Penningtons Manches Cooper LLP (PMC) is a top-ranked UK and international law firm providing advice on cyber security and cybercrime. PMC lawyers are leaders in the field; they recognised cyber law as a distinct and emerging legal specialism at a time when its parameters were first being defined. PMC's practice consistently offers clients both technical excellence and a practical understanding of the key issues.

Close collaboration between the PMC data protection and privacy, reputation management, commercial dispute resolution and white-collar investigations teams ensures PMC lawyers can bring their knowledge and experience across the vast spectrum of civil, criminal and regulatory law as it applies to this area.

Given the potentially far-reaching international exposure of cyber-attacks and data breaches, clients can benefit from PMC's multi-jurisdictional expertise and on-the-ground support from our offices and across our international network of law firms.

As well as being "on call" with a crisis response team for when a cyber-attack strikes, PMC's consistent message to the market is that prevention is better than cure regarding cyber security. On the preventative side, PMC works closely with a wide range of clients to ensure they are well-placed to mitigate the effects of a cyber-attack and respond appropriately when under attack.

These measures often include:

- Assisting with technical audits of systems and infrastructure and identifying potential vulnerabilities.
- Carrying out data audits to understand types of data, data flows and hosting arrangements.
- Recommending penetration testing and simulated attacks to stress test infrastructure.
- Drafting specific cyber security and resilience policies, including to establish an incident management team (with roles & responsibilities) and a practical response plan to mitigate damage and minimise business disruption.
- Reviewing supply chain contracts and drafting robust contracts with cyber security schedules.
- Data protection audit and compliance programs.
- Training directors and staff so that they understand security obligations and can spot the warning signs of cybercrime.
- Reviewing insurance arrangements and assisting with considerations around specific cyber insurance; and
- Advising on regulatory obligations and reporting requirements.

PMC also offers advice on the following:

- Employee liability and protection.
- Data security.
- Control mechanisms for embedded devices.
- Compliance and regulation.
- Preventative measures and policies.
- Data breach response.
- Commercial espionage.
- Investigation of incidents.
- Cyber security disputes.
- Cyber crime prosecutions; and
- Supply chain audit and contract reviews.

Charlotte Hill
Partner

Oliver Kidd
Partner

Tom Perkins
Associate

Charlotte Allan
Trainee Solicitor

Link11: a specialised European IT security provider in the field of cyber-resilience

Link11 is a specialized European IT security provider protecting web services and infrastructures against cyber-attacks. Headquartered in Germany, Link11 maintains global locations, including in Europe, North America, and Asia. The company's cloud-based IT security services help customers avoid business disruptions and strengthen the cyber-resilience of their business networks and critical applications.

Link11's product portfolio includes a wide range of security services, such as web and infrastructure DDoS protection, Bot Management, Zero-Touch WAF, and Secure CDN Services. According to unanimous analyst opinion (Frost & Sullivan, Gartner a. o.), Link11 offers high-performance mitigation across all layers and for all attack vectors, including unknown ones, within seconds.

The technological basis for this is Link11's patented DDoS protection, which relies on machine learning and consistent automation. The company's global multi-terabit network, which currently has 41+ PoPs (Points of Presence), interconnects the DDoS filter clusters, and is monitored 24/7 by the Link11 Security Operations Center.

The German Federal Office for Information Security (BSI) recognizes Link11 as a qualified DDoS protection provider for critical infrastructures. With ISO certification 27001, the company also offers high-level data security processes. Since being founded in 2005, Link11 has received multiple awards for its innovative solutions and business growth.

Contact

Jurij Zykov
Account Executive

j.zykov@link11.com
+49 69 58004926-305

Charlotte Hill
Partner

charlotte.hill@penningtonslaw.com
+44 (0)20 7457 3107

Oliver Kidd
Partner

oliver.kidd@penningtonslaw.com
+44 (0)1483 411404

Sources

[1] https://www.privacyaffairs.com/uk-government-institutions-ddos-attacks/

[2] https://digital.nhs.uk/cyber-alerts/2022/cc-4002

[3] https://www.computerweekly.com/news/366543473/BlackCat-gang-claims-cyber-attack-on-Barts-NHS-Trust?utm_campaign=20230704_BlackCat+gang+claims+cyber+attack+on+Barts+NHS+Trust&utm_medium=email&utm_source=MDN&source_ad_id=366543473&asrc=EM_MDN_271376517&bt_ee=0MDytKE4qcOo5%2BsFJLjKqyPzOrvd9A4oFrGrqXFfCuV3e43z5Rbv%2BEQ69ZRve9Ap&bt_ts=1688466534106

[4] https://www.weforum.org/agenda/2023/01/cybersecurity-storm-2023-experts-davos23/

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf

[6] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

[7] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

[8] https://www.legislation.gov.uk/uksi/2018/506/schedule/1/made

[9] https://www.handbook.fca.org.uk/handbook

[10] https://www.prarulebook.co.uk/rulebook/Home/Rulebook/04-07-2023

[11] https://www.handbook.fca.org.uk/handbook/SUP/15/3.html

[12] https://uk.newsroom.ibm.com/2022-02-23-IBM-Security-Report-Energy-Sector-Becomes-UKs-Top-Target-for-Cyberattacks-as-Adversaries-Take-Aim-at-Nations-Critical-Industries

[13] https://www.theguardian.com/business/2022/sep/06/go-ahead-cyberattack-bus-services-thameslink-rail

[14] https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it

[15] https://www.ncsc.gov.uk/news/ncsc-warns-of-emerging-threat-to-critical-national-infrastructure

Contact

Link11 GmbH
Lindleystr. 12
60314 Frankfurt

www.link11.com