WHITE PAPER

WHY CRITICAL NATIONAL INFRASTRUCTURE (CNI) PROVIDERS NEED CNI-READY DNS SECURITY

NOMINET
CYBER
SECURITY

Executive summary

Most organisations claim that cyber security is a top priority: 74% in the case of UK businesses. But when it comes to critical national infrastructure (CNI), the stakes don't get much higher. According to the Centre for the Protection of National Infrastructure (CPNI), any loss or compromise of CNI services would lead to "severe economic or social consequences or ... loss of life." The 2017 Global Risk Report published by the World Economic Forum highlights "large-scale cyberattacks or malware causing large economic damages, geopolitical tensions, or widespread loss of trust in the internet" as the number one business risk in North America.

There are thousands of CNI operators across the UK and US, running everything from healthcare and energy to transport, emergency services, water and even digital infrastructure. As digital investments improve business agility, operational efficiency and service delivery, they also expose these firms to an unprecedented threat from cyberspace. The US has already faced disruption to its critical infrastructure, while it is a case of "when, not if" the UK follows suit with a so-called category one (C1) attack, according to the head of the National Cyber Security Centre (NCSC).

For too long "security by obscurity" has been the watchword for security teams. But now systems are online and hooked up to the public-facing internet, there is increasingly no place to hide.

The Domain Name System (DNS) layer is at the heart of the problem and the solution for CNI operators. Police this level of your IT infrastructure effectively and you stand a great chance of mitigating cyber-threats and improving resilience. But left untended it could provide hackers with a ready-made channel for delivering malware, denying service and stealing data.

Providers of critical infrastructure therefore need a partner they can trust, to guide them through the minefield of risk management in the digital age. For over two decades Nominet has been running the .UK Registry, using its in-house DNS security platform to protect part of the UK's critical infrastructure. We understand the needs of CNI providers better than anyone and have the tools to hand to help you protect mission critical systems and support digital transformation.

Let's explore some of the key challenges facing CNI providers, and how DNS Security can help face down cyber-risk in an increasingly digital world.

The digital revolution

The critical infrastructure sector has in many ways come late to the digital revolution sweeping the globe. The UK's healthcare system has struggled for years with funding issues, while utilities on both sides of the Atlantic have historically viewed digital transformation as a threat to their business model, according to McKinsey. That is changing today, as cloud-driven platforms open up new IT and business efficiencies, enabling players to innovate their way to growth and competitive differentiation. For example, global transportation ($85 billion) and utilities ($73 billion) firms will spend more on IoT-related technologies than any other sector bar manufacturing, according to IDC.

According to IDC, the top two industries forecast to spend most in IoT related technologies are global transportation ($85 billion) and utilities ($73 billion)

Yet among many CNI providers there's a concurrent challenge: while they're becoming smarter and more connected than ever before, decades-old industrial control systems remain. These monolithic SCADA systems are mission critical in certain environments but run on legacy platforms that can't easily be updated. As a result, their firmware is packed full of flaws, and even communication protocols may lack suitable authentication or encryption. One vendor claimed that it takes on average 150 days for SCADA vendors to release security patches, leaving organisations exposed for around a month longer than for popular software like Windows.

Critical bugs like these are being found all the time. But many IT administrators either rely on perimeter-based approaches which fail to stop more advanced threats, or else try to air-gap systems from the internet altogether — another imperfect solution.

CNI under attack

The result has been a growing spate of successful cyber-attacks on CNI providers. An FOI request sent recently to UK CNI firms found that 70% had suffered IT service outages over the past two years and over a third (35%) of these incidents were caused by online attacks.

A Freedom of Information request sent recently to UK CNI firms found that 70% had suffered IT service outages over the past two years and over a third (35%) of these incidents were caused by online attacks.

Most recently, The UK's National Cyber Security Centre (NCSC), the FBI and the Department of Homeland Security (DHS) released an unprecedented joint alert warning of malicious Russian state-backed activity targeting CNI providers. It claimed:

"Russian state-sponsored actors are using compromised routers to conduct spoofing 'man-in-the-middle' attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations."

It's just the latest of an increasing spate of warnings from national governments and the cyber security industry detailing mounting attacks on the sector. A US presidential report from 2017 claimed that cyber-attacks on critical infrastructure are now as much of a threat as physical attacks. Most worryingly, it stated: "Our response to a large-scale, cyber-attack with physical consequences on critical infrastructure today is likely to be insufficient."

As the global supply chain for critical infrastructure providers continues to expand and increase in complexity, this too will create additional risk: more endpoints for hackers to target, and more user credentials to steal, phish or crack. The NCSC and National Crime Agency claimed in their 2017 report:

"When done well, supply chain compromises are extremely difficult (and sometimes impossible) to detect. Network monitoring can detect unusual or suspicious behaviour, but it is still difficult to ascertain whether a security flaw has been deliberately introduced (possibly as a backdoor) or results from a careless error on the part of developers or manufacturers – or indeed to prove that any potential access has been exploited. Services of almost any sort can be affected, particularly if they involve electronic connectivity or data import."

In short, attackers could target CNI providers IT and OT systems to:

- Disrupt/deny services via DDoS or ransomware: WannaCry ransomware is said to have caused disruption for more than a third of NHS England, with an estimated 19,000 operations and appointments cancelled

- Target theft of IP or customer data: 24% of healthcare organisations have had sensitive customer information stolen (EfficientIP)

- Manipulate or sabotage equipment: suspected Russian state attacks on Ukrainian energy providers in December 2015 and 2016 caused power outages for hundreds of thousands.

- Conduct long-term surveillance of networks, looking for structural weaknesses and other intelligence: FireEye claims to have observed long-term intrusions into industrial control systems "which were not ultimately used to disrupt or disable operations. For instance, Russian operators, such as Sandworm Team, have compromised Western ICS over a multi-year period without causing a disruption."

The need for regulation

This is why the European Commission has drawn up a new regulatory framework designed to improve baseline security among providers of "essential services": the NIS Directive. Unlike the GDPR, it will not apply to organisations outside the EU, but its requirements could serve as a useful reference point to CNI operators elsewhere.

UK CNI firms should be aware that the legislation will be enforced by the government after Brexit. Maximum fines of £17m or 4% of global annual turnover will be levied for serious infractions. According to Corero Network Security, if maximum fines were imposed on UK CNI firms that experienced a cyber-attack over the past two years, it would have cost the economy £2.5bn.

As a provider of critical infrastructure, Nominet fully complies with the NIS Directive.

As a provider of critical infrastructure, Nominet fully complies with the NIS Directive.

Focus on DNS Security

Like many of their counterparts in other sectors, CNI firms are looking to leverage the power of digital investments to enhance business and IT agility, and in so doing differentiate and improve their service. Over half (57%) of global utilities firms have a fully implemented IoT strategy, for example.

However, by going digital, they're also exposing themselves to more threats. The DNS layer offers both challenges and opportunities in this area.

What is DNS?

DNS is a vital part of any network. It is the technology standard used to turn the domain names humans type into their address bar into the internet protocol (IP) addresses understood by machines. Without the DNS, it wouldn't be possible for users to quickly and easily access websites, applications and devices online.

Organisations with a major online presence usually run their own DNS server. Recursive DNS resolvers intercept all outgoing queries to the internet from your employees. This could be something like clicking on a link to connect to a website. To find the IP address of the server that hosts the requested website, the recursive DNS resolver either forwards the query on to other servers or, if it has received the answer previously and cached it, it replies to the user right away. You'll also be running an authoritative nameserver, which maps your domain names to IP addresses of the servers that host them and returns the right results to any external visitors/customers.

The DNS threat

The DNS was designed to be open and accessible to all. Unfortunately, that also means cyber-criminals and nation state hackers, who increasingly regard it as an ideal channel for multiple cyber-threats. Another risk stems from its always-on nature: because it's designed to run in the background, IT administrators can sometimes be guilty of simply ignoring DNS. Most firewalls whitelist DNS traffic, even though there are multiple vulnerabilities in the protocol that could be abused. Almost all cyber-attacks use DNS at some point in their lifecycle, according to the NCSC.

The DNS was designed to be open and accessible to all. Unfortunately, that also means to cyber-criminals and nation state hackers.

Here are the main threats:

1) Changing the answers to the queries stored by your DNS server can redirect users to a malicious website, leading to infection with ransomware, trojans or other malicious code. Users could also be taken to a phishing site designed to socially engineer them into handing over work log-ins or other sensitive information. Redirection can also be achieved by registering a malicious domain that differs only slightly from the legitimate one and the tricking users into visiting. This is known as "typosquatting".

2) Secret, unauthorised transfers of confidential data can happen through DNS. This is known as data exfiltration. "DNS tunnelling" techniques can be used to steal data without detection. There are several, readily available tunnelling tools available online that require little technical expertise to use, with estimates claiming that over 40% of enterprise networks contain evidence of DNS tunnelling. According to Cisco, over 91% of malware uses DNS channels to communicate with C&C servers, exfiltrate data from victims, or receive new commands to attack networks.

3) Denial of Service (D oS) attacks can overload your DNS servers and shut down DNS resolution for a network. This means that queries from real users trying to connect do not resolve and the website crashes. DDoS attacks are increasingly used as a distraction while information-stealing attacks are launched.

Almost all cyber-attacks use DNS at some point in their lifecycle, according to the UK National Cyber Security Center.

CNI protection from a CNI provider

Fortunately, there is a solution. The always-on DNS layer may not have been designed with security in mind, but it provides an excellent strategic location from which to monitor traffic, block threats and keep key data and systems safe and secure.

[the DNS] provides an excellent strategic location from which to monitor traffic, block threats and keep key data and systems safe and secure

Nominet has been providing DNS services for over two decades and runs a full DNS management service to protect the UK government and Public Service Network-connected organisations from malware, phishing, botnets and other threats. Not only that, but as the official .UK Registry for many years, Nominet is also a provider of CNI. Nominet's NTX platform has therefore been designed from the ground-up specifically with the needs of CNI protection in mind.

Based on over 20 years of national-scale DNS expertise and eight years of dedicated research, we have a unique insight into cyber threats, and the capability to find and fix problems that no other service can touch. Out of this experise, the Nominet's NTX platform was born. Our unique, patented compression and analysis algorithms, derived from the fields of acoustics and holography, allows us to capture, understand and visualise the threats contained in your DNS traffic.

Nominet's NTX platform is capable of analysing large volumes of data in real-time to identify suspicious inbound or outbound traffic. The platform is also cloud-based for fast deployment, ease of use and zero maintenance, and can be integrated seamlessly into existing risk mitigation strategies, SIEM solutions and reporting systems.

Plug security into the DNS layer and you get protection that traditional solutions, like AV and network firewalls, might miss, making the DNS a formidable first line of defence.

Nominet's NTX platform is capable of analysing huge volumes of DNS data to provide essential real-time insight into inbound and outbound traffic. By cross-referencing traffic with security lists, it can reveal any infected machines on your network, such as those that have become part of a botnet, or those contacting a command-and-control domain after they've been infected with malware. We can also detect unfolding DDoS attacks from the start, providing all the information you need to mitigate the threat quickly and effectively.

Nominet helps you detect and block DNS threats:

- Malware
- Phishing
- Botnets
- Cryptomining
- Data exfiltration
- Misconfigurations

Choose Nominet Cyber Security managed services for:

Threat assessments and response

Analysis of your DNS network and traffic patterns to the types of threats that your organisation is targeted with, as well as address any potential latency issues.

Protection at the DNS layer

Predictive analysis and expert recommendations to avoid or mitigate the damage associated with cyber-attacks resulting from malware, phishing, botnets, DDoS attacks, spamming, spoofing and cache poisoning, data exfiltration via DNS Tunneling.

Protection Strategies

Work with you to implement and continuously improve your defensive strategies, disrupting the attacks at the earliest opportunity and limiting the business and reputational damage.

Post-breach investigative analysis

Analysing external and internal anomalous behaviour to provide situational assessment, tracing the origins of the attack at the DNS layer, performing a root cause analysis and producing a detailed incident report and recommendations.

Benefits with Nominet

Twenty years of DNS experience: As the .uk domain registry, we use our own DNS security platform to protect our critical infrastructure.

Realtime protection without compromising performance: Purpose-built storage and retrieval platform, allowing you to view and manipulate data in real-time with no maintenance or time-consuming upgrades.

Unique security analytics: A web dashboard fed with unrivalled intelligence , that alerts you to and actively blocks cyber attacks.

A fully managed service: Our team of experts can handle the detection and blocking of cyber attacks and supply you with executive reports, allowing you to work on solutions instead of trying to understand the problem.

Easy-to-deploy security: Can be set-up in minutes with no cumbersome endpoint roll-out. Integrates seamlessly into existing SIEM solutions and management reporting systems.

For more information on how Nominet can help secure your business, please contacts us on:

UK: +44 (0) 1865 332 255
USA: +1 267 908 3004
Email: cybersecurity@nominet.uk
www: nominet.uk/cyber

Sources:

https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
https://www.weforum.org/reports/the-global-risks-report-2017
https://www.cpni.gov.uk/critical-national-infrastructure-0
https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin
http://digitalhealthage.com/nhs-still-struggle-adopt-new-innovation/
https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/the-digital-utility-new-opportunities-and-challenges
https://www.idc.com/getdoc.jsp?containerId=prUS43295217
https://www.infosecurity-magazine.com/news/scada-hmi-devs-take-150-days-to/
https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/dos-injection-flaws-among-vulnerabilities-found-in-ics-scada-routers
https://www.infosecurity-magazine.com/news/a-quarter-of-uk-cni-firms/
https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government
https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08–15–17–508.pdf
http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file
https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
http://www.efficientip.com/wp-content/uploads/PR_DNS_Threat_Survey_2017.pdf
https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack
https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://www.ncsc.gov.uk/guidance/introduction-nis-directive
https://www.wi-sun.org/index.php/news/214-pr-5-dec-2017
https://www.ncsc.gov.uk/information/active-cyber-defence-one-year
https://www.computerweekly.com/news/450303470/Evidence-of-DNS-tunnelling-in-two-fifths-of-business-networks
https://umbrella.cisco.com/blog/2016/01/21/cisco-security-report-more-orgs-should-be-monitoring-dns/
https://hello.neustar.biz/201710-Security-Solutions-Siteprotect-DDoS-2H2017-Report-LP.html

NOMINET
CYBER
SECURITY

For more information on how Nominet can help
secure your business, please contacts us on:
UK: +44 (0) 1865 332 255 | USA: +1 267 908 3004
Email: cybersecurity@nominet.uk | www: nominet.uk/cyber