ASSOCIATION FOR ROAD TRAFFIC SAFETY AND MANAGEMENT

GUIDANCE DOCUMENT

WG3 FEB 2024

PROVIDING GUIDANCE TO MANUFACTURERS AND USER COMMUNITIES

GUIDANCE ON CYBER SECURITY FOR TRAFFIC EQUIPMENT

Introduction

The National Cyber Security Centre defines its Cyber Assessment Framework (CAF) for organisations to mitigate and reduce the risk of Cyber attack. CAF was developed for the UK Government and all government departments must assess against the Framework. It was built for large organisations but has expanded its usage beyond its initial assessment only criteria. However, it is intended to provide the user with outcomes, not how to achieve them. It provides useful guidance for all levels of business, including SMEs and sole traders. Manufacturers should consider cyber security at all stages in the lifecycle of their products and services. Users may want to focus on the operation and maintenance phases of the lifecycle.

Traffic industry products

The key point above is risk. Within the traffic industry we generally have fixed pass/fail criteria in engineering – e.g. the timing is 5s +-0.2s, does it work at 60C to -15C?

Cyber security protection is ensuring you have identified potential risk and taken steps to mitigate such risk. The key to this risk assessment is to address risk across the ecosystem of the traffic industry.

For the purposes of this Guidance equipment on street such as traffic light controllers, detector outstations, variable message signs, etc. will be called 'outstations'. Any router, media converters and networks will be called 'communications equipment' and any central systems will be called 'in-stations'.

We tend to think of cyber security as only being anything connected to the internet but consider that even equipment not connected to the internet can be vulnerable to cyber attack. Most outstations and communications equipment in the traffic industry now operate using an operating system akin to your laptop and are at the same risk of hacking and malware as a consequence.

The NCSC publish a risk level and also notify of specific threats. Often the threat level will be increased at certain times, such as the start of the Ukraine war. You are also able to report threats you have identified. It is advisable that you maintain regular checks from the NCSC website.

Business Processes

Traffic equipment companies themselves can be prone to cyber security issues, this could result in an interruption to business which includes supporting customer and products. Companies should therefore consider external certification Cyber Security Essentials provides companies with a basic technical assessment of their protection while the Plus standard provides an independent assessment, while ISO27001 provides an additional step in protection.

These processes help provides companies to ensure continuity of operation and service but also help protect traffic equipment. Issues that can arise a developer's PC could be infected with malware and infect the software and OS being developed for a piece of traffic equipment. Software could be transferred on an infected USB drive, an engineer could be have downloaded a file at home that is malware and then the next day connect to the traffic equipment outstation and infects the equipment.

These processes will also cover what to do in case of a malware attack or security vulnerability and this will include informing those affected including users and customers.

The certification processes suggested here firstly help to prevent any cyber security issues, but then also address business continuity, reporting and resolution of cyber attack issues.

Offshoring should also be considered many companies now subcontract software development to companies around the world, how are these companies and their staff vetted are you paying for malware.

Product and Service Development and Maintenance

Cyber-security should be considered at all stages in the life-cycle of a product or service, selecting platforms, operating systems, architectures, etc. that are robust and resilient.

Consideration also has to be given to applying a proportional level of cyber-security which suggests that a risk assessment and mitigation should form part of this design process.

Manufacturers should consider cyber security at all stages in the lifecycle of their products and services. Users may want to focus on the operation and maintenance phases of the lifecycle. This guidance is intended to offer areas for consideration so that everyone with an interest in cybersecurity can develop and evolve their products, services, work processes, etc. with the objective of achieving an appropriate and proportionate level of mitigation against cybersecurity threats.

Outstations

Most traffic equipment outstations run on an operating system, often PC derived, which provides a good point of cyber attack. Remember with engineer visits or developers, equipment does not have to be connected to the internet to become infected. Plugging into a communication port or using a USB drive are all good points of access.

All outstations should be protected for cyber security typically this will look to penetration testing, during the development phase. All communication and diagnostic connection points should be protected and non-secure ports protected or closed. Often engineers will use open services such as Telnet or File Transfer Protocol for development and diagnostics, these should be updated to protected versions or closed prior to release. Given the specific nature of cyber security independent assessment and testing “Penetration Testing” is recommended using third-party expert services. This should assess the equipment against a variety of common threats and grade the risk against each area of concern and report accordingly.

When considering an Operating System care should be taken to ensure it receives updates for published security vulnerabilities, this provides the developer the opportunity to provide security patches or updates to equipment as threats evolve. Due to the fast-changing nature of Operating Systems it should be considered looking for a long term support version as traffic equipment can be in the field for 10-15 years and this reduces software development effort moving from one version of operating system to the next.

Consideration should be given to remote software updates to deploy security patches or software updates to protect against a security vulnerability rather than waiting for annual maintenance visits. This also needs to be considered when maintenance of traffic equipment may change every few years. Consideration needs to take into account traffic specific requirements so considering Traffic Controllers and level 3 access requirements security patches would need on-site support.

Physical and security protection also needs to be considered, having street cabinets with common locks is very flexible for maintenance but you would not provide one password to use for everybody in the organisation. Remember opening a cabinet not only provides access to the outstation but also free access to the communications equipment.

Webservers provide an excellent tool for user access to outstations for monitoring and control these should be password protected and the password should be unique and complex, rather than the whole county using one simple password. This requirement needs to be carefully considered against best practice and the requirement of maintenance staff working across a large number of assets.

Wireless transmission, especially for maintenance, provides excellent a very convenient communications path. Considering Wi-Fi if in constant use it provides an easy path to be hacked, so passwords should be unique and Wi-Fi should not be operating when nobody is in attendance. There are differing views on the validity of changing passwords, particularly in organisations that have significant numbers. In principle, all passwords should be set at the highest level of protection at the outset.

Communications

Routers and media converters connecting outstations to networks again should be considered in much the same way as the PC in your office and are at risk of malware attack. The simplest attack is to open the street cabinet and plug into the network. This may simply result in a free use of the network running up mobile data charges or could be used for a malware attack. Once again you should consider physical protection to communications equipment, cabinets on street with simple or common locks make easy targets for access.

Routers will have password protection. These should be changed from the default and use unique complex passwords. Routers have also been known to be susceptible to malware and this can be transmitted from router to router if the network allows. This requirement needs to be carefully considered against best practice and the requirement of maintenance staff working across a large number of assets.

Some users will have private networks connecting their offices to equipment on street. Firewall and routing rules should prevent equipment at street level talking from one to another risking infection. It should also be noted that if this equipment has users PCs on the same network particularly an office environment then the condition for “Development and Maintenance” should be considered in case an office PC infects an OS on traffic outstation. This requirement of best practice needs to consider where assets are linked through IP connections locally such as linked MOVA or remote I/O which need these local links to function.

When considering public networks protection is more key, all traffic should be encrypted and the use of a VPN Tunnel (Virtual Private Network) considered. This provides a secure encrypted connection between the in-station and the communications equipment on street.

Mobile communications provide a very easy way to connect equipment on street and reduces infrastructure required to deploy equipment especially in rural areas. A Public Static SIM is ideal it provides a fixed IP address that can be accessed anywhere, so this is a good target for remote hacking, so should be avoided. All SIMs used should be protected ideally operating over a private APN with an agreed and secure access point. Once again routing should prevent one SIM being able to talk to another to prevent malware transfer. Once again a data traffic should be encrypted and a VPN tunnel should be considered to encrypt and protect access to specified endpoints.

In-Stations

All the comments above about the need to consider cyber-security for the whole product and service life cycle apply equally to in-stations.

The effects of malware, hack or denial of service, or other cyber-attack will have most effect during the operational phase of any product.

As noted above, some users will have private networks connecting their offices to equipment on street.

Consideration should be given to segregation of office-based PCs that access traffic systems from the general local authority or business IT networks. If in-station equipment has users' PCs on the same network, particularly in an office environment then the risks that this presents, particularly of an office PC infecting an OS on a traffic outstation, should be addressed in the development, maintenance and use of the in-station.

Applying the NCSC guidance will go a long way towards improving the cyber-security of in-stations.

Gap analysis

When considering cyber security, in the same way as other risk areas in your business, you should undertake a risk analysis. We recommend that you apply the UK Cyber Assessment Framework (CAF), which was developed for use by all government bodies.

The CAF provides a very useful framework to undertake your risk gap analysis. You should consider all areas of business, as above, including basic GDPR and other UK legislation which relates to your company.

What are you required to provide by your customers?

What are you company insurance requirements?

What are the relevant requirements for your business?

There are two main routes to gain accreditation for Cybersecurity in the UK to consider, once you have completed your gap analysis:

Cyber Essentials – government backed and recognised by NCSC

ISO 27001 – also supported by government

Both of these draw heavily on NIST from the USA.

These processes cover what to do in case of a malware attack or security vulnerability and this will include informing those affected including users and customers.

The certification processes suggested here help to prevent any cyber security issues and also address business continuity, reporting and resolution of cyber attack issues.

As part of your cybersecurity analysis you should ensure you establish which of these accreditations works best for you.

Useful links

Cybersecurity Framework | NIST – NIST now using NIST 2

CIS Center for Internet Security (cisecurity.org) – USA system

NOTE : CIS has 18 controls whilst NIST has 105 – however there is a 95% overlap on the standards.

About Cyber Essentials - NCSC.GOV.UK – UK system Government backed accreditation – recommended for all SMEs and sole traders as well as large companies

ISO 27001 – process driven accreditation – checklist can be downloaded to assist in understanding content of standard.

NCSC CAF guidance - NCSC.GOV.UK – Cyber Assessment Framework – UK government backed – initially built for large organisations. All government bodies assess themselves against this framework. Gives you expected outcomes, but now how to achieve them.   CAF was derived from NIST.

BT launches new Managed Security Service to protect UK firms as they face cyber-attack every 45 seconds

Government Cyber Security Strategy 2022–2030 (publishing.service.gov.uk)

DIRECTIVE (EU) 2016/ 1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 6 July 2016 - concerning measures for a high common level of security of network and information systems across the Union (europa.eu) – NIS

Publications Office (europa.eu) – NIS2

Acronyms

NIST – National Institute of Standards & Technology, USA

NCSC – National Cyber Security Centre, UK

CAF – Cyber Assessment Framework, UK

CIS – Centre for Internet Security, USA