SAFETY FIRST

Fabian Libeau *reveals how an inventory of attack surfaces guards against cyber-attack*

In its review of 2021, the National Cybersecurity Centre (NCSC) highlighted not just the rise in ransomware attacks against public and private organisations, but also increased hostile acts targeting critical national infrastructure and government. A memorable example was the attack on software giant SolarWinds and the exploitation of Microsoft Exchange Services, which affected the supply chains of government, economic and national security bodies. Tens of thousands of US institutions, including the Treasury, were affected, but cyber warfare is fought on the global stage and the UK also felt the impact, not least on British security firm Mimecast, which had its source code stolen because of the SolarWinds breach.

National critical infrastructure is particularly at risk from the international escalation in cyberattacks. It encompasses everything from emergency services, healthcare, energy and water through to transport, communications and civil nuclear. We might think that our lives depend on our mobile phones and laptops, but if access to electricity were to fail, our bank accounts were shut down, food deliveries were disrupted or we couldn't trust the water flowing out of our taps, that could have much more damaging significance. Protection of this infrastructure – the property, networks, information, people and processes that it encompasses – is essential and more vulnerable with every day that passes.

Right now, following events in Ukraine, we face an escalation in cyber warfare that has put all organisations onto high alert. In the US, the White House's Deputy National Security Advisor for cybersecurity and emerging technology proactively ran a tabletop exercise to ensure federal agencies were prepared for the likelihood of cyberattacks from Russia having a greater focus on any NATO nation voicing strong opposition to its actions. In the UK, local councils are being encouraged to take rapid action to protect their systems while the NCSC says the threat of a cyberattack is: "heightened".

There are practical steps that organisations whose services we rely on can take to shore up their defences. The most obvious is to increase their security awareness, which means alerting staff members so they can be more aware of what suspicious activity looks like. An unexpected email with an attachment or a link urging them to open it should be treated with caution and reported. IT, operations and security teams must pay attention to logs and system monitoring tools for increased login attempts, unusual behaviour or increased outbound traffic. If they assess what normal looks like – bearing in mind the changes brought about by 'hybrid working' – they will be able to more clearly see a change. Security teams should be alert to threat actors hiding in plain sight, which could mean they take control of dual-use technologies and processes like PowerShell or PS Exec, for example. Knowing their organisation's systems, processes and applications and continuously monitoring them will allow them to identify deviations quickly. If the organisation has not already adopted multifactor authentication or passwordless authentication, now might be a good moment to revisit these capabilities. Another tip is to consider implementing Zero Trust, which by definition means that all access and authentication must be verified first. This is also an effective way to mitigate the threat of endpoint devices that are unsecured and which, because of the proliferation of hybrid and remote work, present a threat to organisations. Protecting these devices is a must.

Legacy technology – which still underpins much of the critical national infrastructure in the UK – is often insecure and outdated

The challenge of preparing to fight against a cyberattack will always be very different to preparing traditional warfare defences because stealth lies at the core of these attacks. We might suspect that an attack has been state sponsored and the attackers are using their country's assets to guard their anonymity, but we don't know for sure. We live in a digital world that is more intricately connected than ever before and it is easy for bad actors, particularly those sponsored by the state, to be covert in order to achieve their missions.

While it's important to attribute attacks to specific groups or governments to increase our learning and build resistance, this should not distract us from the very real impact of the assaults and the operational damage that can be caused to critical infrastructure. Damaging the fabric of vital institutions and economies and degrading our trust in the services they deliver has a knock-on effect on how they support civil society, and this disruption plays directly into the hands of cybercriminals.

Attacks are possible, of course, because many of these essential services are built on highly fragile, often complex, systems. Legacy technology which still underpins much of the critical national infrastructure in the UK is often insecure and outdated. However, more concerning is where legacy systems have been combined with digital technologies that use modern features such as advanced analytics and automation but are not configured to close the many gaps in their security posture.

Added to this are the different priorities of operational (OT) and information technology (IT). OT systems are designed to deliver availability come what may. They run constantly to avoid any interruption that could lead to production delays, so are robust and often open. They are built with safety in mind because engines, motors and processors can present a physical risk to operators. The priority of IT, however, is not physical safety but a secure network to protect the sensitive data that flows across it.

THE EVENTS IN UKRAINE HAVE LEAD TO A SUDDEN AND RAPID ESCALATION OF CYBER WARFARE

The convergence of OT and IT has created a perfect storm in which cyberattacks can proliferate. As new IoT-enabled devices are added to ever-growing IT networks, which in turn are integrated with existing OT systems, it is not only connections that are proliferating, but chinks in what should be a protective armour. All too often there are gaps that leave OT unprotected. A balance needs to be reached between ensuring uptime and building systems that can work in tandem, while being as close to unbreachable as possible.

Incidents of this size and nature tend to sharpen the focus when it comes to protecting the systems we rely on. Inevitably there have been calls to address the gaps that exist in the security posture of important critical infrastructure operators on both sides of the Atlantic, particularly where they relate to OT assets – the physical or virtual digital devices that make up the OT infrastructure.

This, however, is a considerable challenge for security teams who must carefully work to extend the security perimeter to protect OT networks that are built to operate mechanical equipment or power machinery, as discussed earlier. These systems are not designed to be shut down for a security agent to be implemented, even if the necessary software agent is suitable. Negotiating their way around supervisory control and data acquisition systems that control electrical transmission substations, or pumps that push water through a treatment plant, bears little similarity to their usual role of securing and protecting data privacy.

Security teams have the added hurdle of a multitude of legacy and contemporary assets with both proprietary and contemporary protocols. Added to that are the limited resources that could give them valuable information about those assets (memory, processing), constrained and controlled network access, an inability to rely on software agents and network scanners, and a great deal more.

▶

But it is a task that must be faced, and for critical infrastructure operators there are three key steps to take that will help them build defences around their OT assets and networks to protect from cyberattack:

Construct an inventory of OT and IT assets

Security teams aiming to secure OT assets often find it difficult to gain a full understanding of the assets that exist on their OT networks. It might be that the OT assets are running on a platform that is outdated or that it cannot run a suitable endpoint agent or other security solution.

> **THERE ARE PRACTICAL STEPS ORGANISATIONS WE RELY ON CAN TAKE TO SHORE UP THEIR DEFENCES**

In addition, the existence of older systems with proprietary communications protocols increases complexity. A comprehensive inventory of the assets, software and users on OT networks will give security teams new levels of visibility into these critical assets.

Cybersecurity asset attack surface management (CAASM) platforms can help operators by correlating the data collected at the network layer, SCADA historians, device management tools, security agents and more to help gain a comprehensive OT asset inventory without impacting performance of critical infrastructure.

Prioritise areas for improvement

With the asset inventory completed, security teams can then identify where security initiatives will have the greatest impact. For example, they can discover the devices in the OT environment that can and should have a security agent installed, but which are currently missing that agent.

The asset inventory can also help prioritise the assets and devices that should be updated or replaced. Many newer OT assets will be more suitable for supporting modern operating systems and security agents.

Align IT and OT Policies

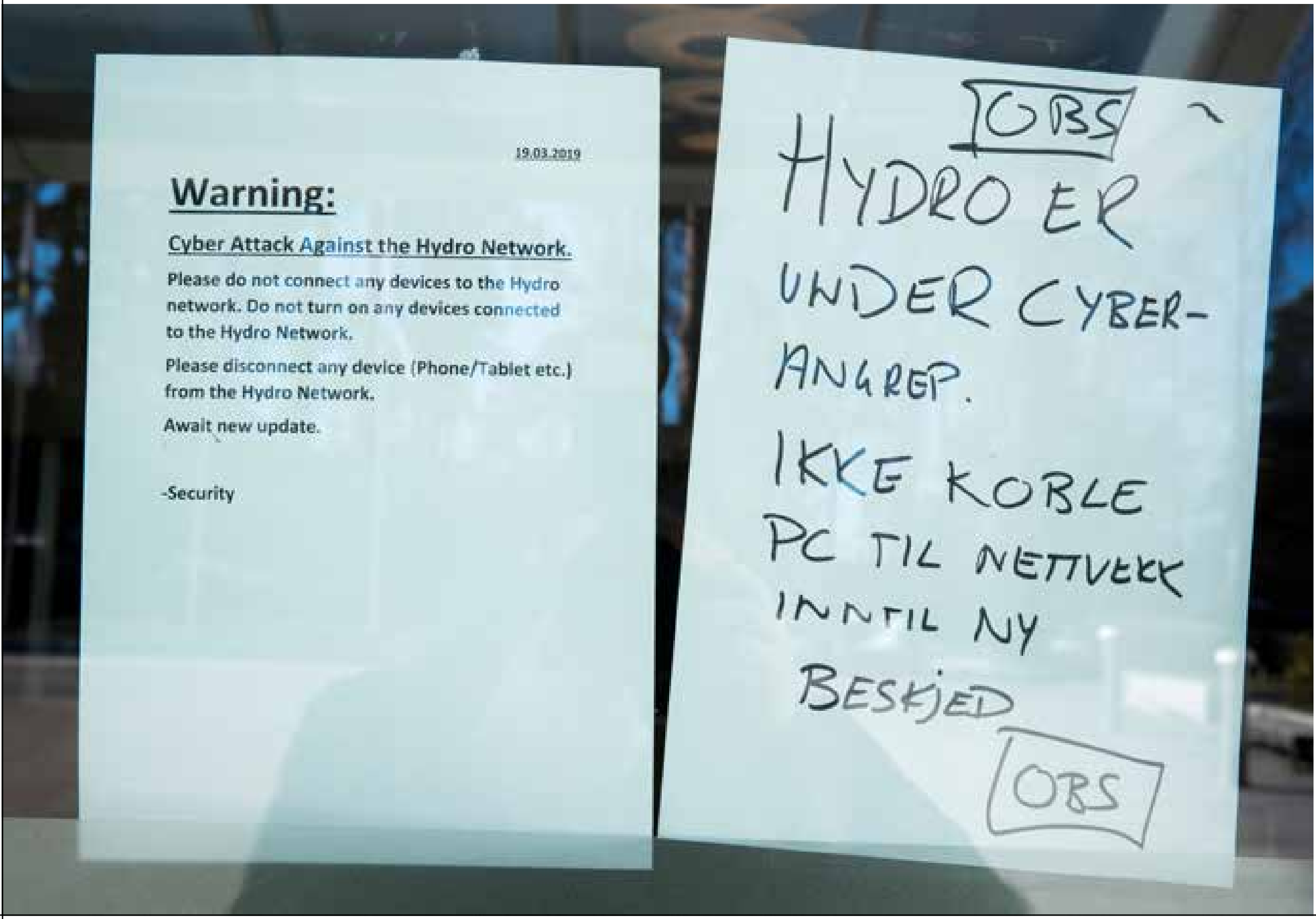
For all the reasons already explained, patching and updating OT assets can be disruptive and security teams must tread carefully. However, finding opportunities to align other standards, policies and tools to the point where they are feasible will up-level the security posture of OT networks and is a critical part of an IT/OT convergence strategy.

A fundamental approach to protecting against the rising tide of cyberattacks is gaining full visibility of everything that might present a risk whether it's an OT or an IT asset. No organisation can secure what it can't see, so developing an up-to-date inventory is essential. This does require CAASM platforms because not only can they find those assets and reveal any gaps in the security defences, but they can also assess whether acknowledged assets meet with agreed security policies.

Keeping national critical infrastructure safe requires platforms that work across all systems and are adept at integrating with existing security, management and operational tools. It doesn't matter if details are being derived from a cloud server, a router on a plant floor or a wi-fi enabled coffee machine, the important factor is that it is recognised and can be protected. Without this level of visibility into attack surfaces, organisations offering vital services will remain vulnerable ●

Fabian Libeau is the VP of Sales, EMEA at Axonius. He brings more than 20 years of building cybersecurity business across EMEA. Prior to Axonius, Fabian was VP of Sales & GM at RiskIQ in EMEA and built the business successfully, which led to an exciting exit with the acquisition by Microsoft.

> **No organisation can secure what it can't see, so developing an up-to-date inventory is absolutely essential**



19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security

OBS

HYDRO ER UNDER CYBER-ANGREP.

IKKE KOBLE PC TIL NETTVERK INNTIL NY BESKJED

OBS

Picture credit: Getty