UKAuthority
Public Sector Cyber Forum

20 September, London

Supported by:

splunk>

mimecast

New challenges and opportunities in public sector cyber security

UKAuthority's Public Sector Cyber Forum 2018 produced valuable insights on how new technologies are changing the cyber landscape for public services

A UKAuthority Event Briefing Note

Contents

1. Introduction

New challenges are arising for those dealing with cyber security for the public sector. As authorities aim to harness new technologies such as the internet of things (IoT), artificial intelligence (AI) and augmented reality (AR), it creates new points of vulnerability and risk. These are not yet fully understood, but those in the vanguard of the effort are clear that it makes the assessment of threats and possible weak points even more complex.

This has intensified the need for best practice, sharing experience and intelligence between organisations, and a strong appreciation of the risks among public sector business leaders. Protection requires investment and the effort to create a culture of security, but the threat is often seen as a distant possibility rather than a pressing issue.

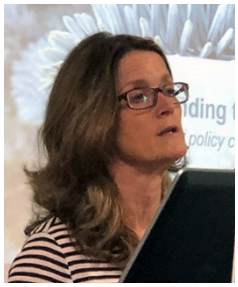
These factors provided the backdrop to UKAuthority's recent Public Sector Cyber Forum, which brought together expert speakers with a core group of public service delegates to explore the issues and priorities for organisations.

2. Changing landscape

While the awareness of cyber threats is now widespread, the understanding of the details is less certain. "Cyber security can mean so many things it almost means nothing," commented Madeleine Carr, associate professor of cyber security at University College London. "Different things can require different outcomes, even conflict with each other."

Harnessing the IoT, AI and AR will demand the aggregation of a massive number of data flows, with the IoT in particular involving the connecting of millions of devices that could each provide a point of vulnerability. It would not be beyond the capabilities of attackers to find ways into a network through a small number of sensors or devices. The point was made that some of these are so small and simple that they could be impossible to secure, but they are also built to last a long time and it would be a major job to replace them if a vulnerability is identified. There would be questions of responsibility and costs that could undermine the drive by local and regional authorities to use the technology in creating smart places.

A group of UK universities are working on research into the issue under the PETRAS programme[1] – which is examining various factors in the application of the IoT – but at the moment it is still an area most organisations are feeling their way forward.



The increasing use of cloud systems is adding an extra dimension. While these are often portrayed as providing a secure environment, they do not automatically make an organisation's whole network secure, with attacks often targeted at different elements of the data supply chain. This can come through other agencies with which it interacts – some of them small with little of their own protection in place – and through emails to staff. David Staunton of

[1] PETRAS programme : http://www.paccsresearch.org.uk/news/petras-cyber-security-research-hub/

Mimecast said its survey of public sector customers showed that almost all had been subject to an email attack in the previous 12 months, and that half were not confident in their organisation's ability to defend against malware/ransomware/phishing mails to come through the channel.

It relates to a specific warning from Staunton that the public sector is attracting increasing attention from cyber attackers as it is handling such a deluge of data, and a perspective that it has not invested sufficiently in IT security.

There are, however, new tools becoming available to reinforce the efforts to defend against attack. Data analytics is becoming increasingly sophisticated and providing the potential to spot irregularities in network traffic and alert an organisation to a denial of service attack. It can help its cyber team to ask questions that attackers would ask, relate them to knowledge about known threats and identify previously unknown vulnerabilities.

The potential is being increased by the application of machine learning: algorithms that can monitor and process a much larger volume of activity than any human and learn from their own observations. This can be used in security and IT operations to predict a potential threat before it takes a clear shape and enable the team to take defensive actions.

Overall, the threats and the solutions are developing at a fast pace, creating a cyber arms race in which the public sector is one of the battlefields.

3. The leaders' issues

Despite this, in many public authorities it is a struggle to keep cyber security on the agenda of top level executives. Nobody denies it is an important issue, but the effort to plan for an effective response is often constrained by other pressures on boards.

Stephen Baker, chief executive of Suffolk Coastal and Waveney District Councils, outlined what hinders the response in terms of other priorities and immediate pressures:

- Lack of skills, knowledge and experience; lack of understanding and awareness.
- The complexity of operations and systems, with a collection or systems, partnerships and users working together.
- It can be difficult to quantify the risks.
- There is a reticence to quantity the impact.
- Denial of the extent of the danger coming from a desire to avoid causing alarm.
- A feeling it is somebody else's issue.
- The political interface, a struggle to convey to councillors the nature of the threat and what needs to be done.

But he argued it should not be pushed aside. "We have a leadership role in terms of getting the message through to communities and stakeholders," he said. "There is a need to provide the lead for advice and guidance."

An element to this is making the messages as simple as possible. Rowena Schoo, senior policy adviser for cyber security and data protection at the Department for Digital, Media and Sport, said that the department is working on a new approach to how it speaks to people about cyber security. Part of this can involve providing the right incentives and regulations, and looking at how it could be possible to benchmark performance on cyber as a first step to improvements.

Baker advocated some steps that an organisation can take to mitigate the threat:

- Carrying out an exercise to think about the possible impacts of a cyber attack.
- Apply a timeline to these, thinking about factors beyond the initial effect on services such as the damage to confidence and reputation.
- Acknowledge the risks.
- Educate staff in the basics of cyber security.
- Bring in the specialist skills, whether they are in-house or with contractors.

A couple more interesting pieces of advice emerged. Andrew McAlister of Splunk emphasised the need to ask 'What if?' questions about an attack on different elements of an IT infrastructure – because that is what the cyber attackers do. Steve Kennett, security director of Jisc, added that there are no stupid questions in cyber security.

4. Research effort

There are some notable areas of research that could feed into all the advancement of effective cyber security in the public sector. Madeline Carr reported on efforts to evaluate evidence on cyber security issues for policy advice. This involves looking at the roles and priorities of people who provide the advice, and assessing their evidence for any bias and the rigour to which it is submitted.

Another is to look at the potential for credible cyber metrics. Organisations need to know whether they are doing a good job, and it would help to be able to quantify what is needed. This needs input from both technology and business leaders to find the right metrics to match their priorities, and to present them in a way that would make sense to both sides. This can be important in helping to push cyber up the organisation's agenda, especially if the metrics can be related to factors such as business continuity, legal liability and return on investment.

The third is to build relationships with research teams overseas. While this may seem detached from the priorities of public authorities in the UK, there is plenty of scope for learning from common experiences in light of both the global threat vector and the fact that authorities in all countries are moving onto new ground with implementation of IoT technology.

However, getting the research out of academia and onto the desks of the officials who could benefit from it is not always easy: Carr made the point that few people want to read peer reviewed articles.

There is a need to relate it to their business priorities and outcomes, but it is difficult to shape this to a wide range of perspectives, even staying within the public sector.

5. Government initiatives

Efforts are taking place to bolster UK government's plans for a response. Siobhan Coughlan, programme manager at the Local Government Association, outlined its stocktake of cyber security arrangements among local authorities. This was being compiled at the time of the event and was aimed at providing an evidence base to from which to both target improvement and push the issue up the agenda in councils.

The other was the 18-month programme of the Resilience and Emergencies Division (RED) of the Ministry for Housing, Communities and Local Government to work with local resilience forums on building up their cyber security capabilities. Alice Reeves, head of resilience for RED, said tha it was about moving cyber away from a 'security box' to thinking about it more in an emergency planning and preparedness space. Access to data and being able to communicate with other agencies is an essential element of any emergency planning, and organisations need to map out these needs as part of their cyber planning.

6. Conclusions

It is a broad, complex landscape and nobody can claim to have a definitive approach to preparing for the inevitable threats, but three strong points emerged from the presentations and conference discussion.

1. One was that public authorities need to raise the bar for suppliers of IT systems. The concept of 'security by design' has now been around for several years, and organisations should have the confidence to demand that any software or hardware they buy has appropriate security measures built in. They have more chance of doing this with a strong influence from central

government or by working collectively, making it clear to suppliers that there are standards that should not be breached.

2. Second is the need to step up the intelligence sharing, not just on prevailing threats but at common issues that arise when weaknesses in their systems are spotted without an attack having taken place. They can look at the settings in systems to significantly reduce a threat and share the steps they have taken with other authorities. This would not be possible for every system, but the growing use of commodity platforms by public authorities increases the scope for it to be effective.

3. Third is the need to bring together the potential in machine learning and other emerging technologies with the effort to instil a healthy cyber culture in an organisation. It will be possible to automate more of the cyber security effort, but the attackers will always look for new approaches and there will always be the danger of people – the human element - providing the weak points that can be targeted.

The mantra of educating staff about the dangers and their responsibilities will remain as important as ever, but it has to done in terms that people can appreciate. Training and awareness raising has to be appropriate, proportionate and complement the business rather than put barriers in the way. Organisations should sell it to their employees as a way of helping them to do their jobs better.

Bringing together the automation and education for strong cyber security will be a big part of the way forward for organisations in all sectors.

7. Partner comment

Gordon Morrison, Director, Government Affairs, Splunk

The presentations and discussions at UKAuthority Public Sector Cyber Security Forum reflect the rapid and complex changes in the cyber landscape.

As public authorities explore the potential of emerging technologies such as artificial intelligence, augmented reality and the internet of things they are tapping into enormous potential. But the explosion in the number of connected devices and sensors, combined with the rising number of connections to cloud services and other organisations' digital systems, is creating a big growth in the number of potential points of vulnerability.

It is opening up an array of opportunities for cyber attackers and multiplying the complexities around the effort to create robust defences.

From Splunk's perspective, an important element of the response is for public authorities to harness the relevant data that they hold and use the talents of people who think in the same way to cyber attackers. They need people who will ask similar questions to the attackers but turn these towards improving their protection, looking closely for weak points not just in an organisation's IT infrastructure and networks, but along its data supply chain to cloud services and connections with other organisations. They will have to ask questions about what could happen if these weak points were targeted in specific ways, and what type of pressures would undermine their network security.

These people need access to vast, real-time datasets on the performance of digital infrastructure, the activity in IT operations and network traffic. Multiple sources of information are available – such as logs from firewalls, malware detection systems and domain controllers – and the emergence of a new generation of data tools and machine learning is making it easier to pull it all together and sort through the mountain of data for analysis.

When they ask questions these tools can provide answers quickly, and lead to new questions about risks and weak points. It can help organisations to better understand their own operations, in terms of the technology, people, processes and expansion of vulnerabilities.

The right type of data platform can provide the capacity for the specialists to do this – to ask questions, test their ideas, fail quickly and safely, and develop solutions that stand up to real world operations.

It is all about using data to strengthen cyber security, and provide safer, more reliable services for the public over the long term.

8. Speakers and their presentations

(Visit the UKAuthority Public Sector Cyber Forum 2018 event hub)

Cyber Security – is it a case of preparing for the inevitable?
Stephen Baker, Chief Executive, Suffolk Coastal & Waveney councils
(Presentation slides (2.5mb)

Cyber Security Policy in an Evolving Landscape
Rowena Schoo, Senior Policy & Comms Advisor - Cyber Security & Data Protection, DCMS
(Presentation slides (8mb)

The two sides of cyber resilience; how to protect your organisation from attack and how to protect yourself from human error

David Staunton, Product Marketing Manager, Customer Strategy, Mimecast

(Presentation slides (13.5mb)

Data at the core of cyber security across three councils

Morgan Rees, Infrastructure Delivery Manager, Surrey County Council/Orbis Partnership

Protecting the next generation from cyber attacks and ensuring schools can operate in all conditions

Michael Eva, Programme Manager, London Grid for Learning

(Presentation slides (18.5mb)

Cyber Security – Jisc's New Approach

Steve Kennett, Security Director, Jisc

(Presentation slides (23mb)

Understanding the Ecosystem

Dr Madeline Carr, Associate Professor in International Relations and Cyber Security, University College London

(Presentation slides (12mb)

Delivering local multiagency cyber resilience – MHCLG cyber plans

Alice Reeves, Head of Resilience & Cyber Projects, MHCLG

James Young, Cyber Resilience Programme, MHCLG

(Presentation slides (1mb)

9. Public Sector Cyber Forum 2018 – Our Partners

splunk>

Thousands of organisations rely on Splunk as the single source of truth to help drive better, faster security decisions.

Splunk User Behaviour Analytics (UBA) not only focuses on external attacks but also the insider threat. Its machine learning algorithms produce actionable results with risk ratings and supporting evidence that augment security operation centre (SOC) analysts' existing techniques for faster action.

Splunk was founded to pursue a disruptive new vision: make machine data accessible, usable and valuable to everyone. Machine data is one of the fastest growing and most valuable parts of big data - generated by every component of IT infrastructures, applications, mobile devices, website clickstreams, social data, sensors and more.

Splunk is the leading software platform for machine data that enables customers to gain real-time Operational Intelligence. Our company's mission is to address the challenges and opportunities of managing massive streams of machine-generated big data. More than three quarters of the Fortune 100 and thousands of enterprises, universities, government agencies and service providers use Splunk software to harness the power of their machine data for application management, IT operations, security, web intelligence, customer and business analytics and more.

Splunk helps customers solve problems in ways they could never dream before. With Splunk, all you need is a browser and your imagination. **www.splunk.com**

mimecast®

Founded in 2003, the company's cloud-based security, archiving and continuity services protect email and improve organizations' cyber resilience with comprehensive email risk management in a single, fully-integrated subscription service.

• Mimecast Email Security protects against malware, spam, advanced phishing, impersonation and other emerging attacks, while preventing data leaks.

• Mimecast Mailbox Continuity ensures employees can continue using email during planned and unplanned outages.

• Mimecast Cloud Archive unifies email, file and Instant Messaging data to support e-discovery, GDPR compliance and gives employees fast access to their personal archive via PC, Mac and mobile apps. **www.mimecast.com**

10. Participants at Public Sector Cyber Forum

10.1 Where they came from

Brighton and Hove City Council, Cambridgeshire Police, City of London Corporation, City of London Police, Department for Digital, Culture, Media and Sport, Dorset HealthCare University NHS Foundation Trust, Ealing Council, East London Advanced Technology Training (ELATT), East Sussex County Council, Eastern Region Special Operations Unit, Essex County Council, Gloucestershire County Council, Home Office, Jisc, Local Government Association, London Borough of Croydon, London Borough of Islington, Looking Local - Co-owned by Kirklees Council, Ministry of Housing, Communities and Local Government, National Offenders Management Service, Northamptonshire Police, Sandwell Metropolitan Borough Council, Solihull Metropolitan Borough Council, Southend Borough Council, Staffordshire County Council, Stevenage Borough Council, Suffolk Coastal and Waveney councils, Surrey County Council, University College London, University of Cambridge, Watford Borough Council, West Midlands Police

10.2 What they do

Associate Professor in International Relations and Cyber Security, Auditor, Chief Executive, Chief Tactics Technician, Cyber and Information Security Lead, Cyber Resilience Programme, Cyber security advisor, Detective Chief Superintendent, Director of Technology & Digital Transformation, Enterprise Infrastructure Delivery Manager, Head of Digital and Data, Head of IT - Projects & Programmes, Head of IT Strategy & Engagement, Head of MIS, Head of Resilience, Information & Records Governance Manager, Information Assurance Team Manager, Information Governance Officer, Information Security & Governance Manager, Information Security Officer, IT Infrastructure Project Manager, Manager, Permit policy, Blue badge and Fraud, Managing Director, NFIB Cyber Protect Officer, Principal Business Continuity Officer, Programme Manager, Regional Cyber Prevent Coordinator, Researcher, Resilience Officer, Security Architect, Security Director, Senior Developer, Senior Policy and Communications Advisor - Cyber Security & Data Protection, Systems Expert, Technology Development Officer, Vendor & Partner Liaison Analyst, Web content designer

11. Forthcoming UKAuthority events

Book your place at March of the Bots 2018

Book your place at Digital Health & Social Care 2019

Book your place at Cyber4Good 2019

To discuss speaker and sponsor opportunities contact Helen Olsen Bedford: helen@ukauthority.co.uk