APPG ON CYBER SECURITY MEETING ON CYBER SECURITY

MINUTES OF THE APPG on Cyber Security 18th December 2017

Chair: Vicky Ford MP

Location: Committee Room 16, Houses of Parliament

Time: 16.00 – 17.30

Present:

Lord Hodgson of Astley Abbots

Baroness Neville-Jones

George Howarth MP

James Morris MP

Richard Benyon MP

Apologies:

Lord Arbuthnot of Edrom

Lord West of Spithead

Speakers:

Professor Keith Mayes, Information Security Group, Royal Holloway

Dr Daniele Sgandurra, Information Security Group, Royal Holloway

Declan Hadley, Digital Lead, Lancashire and South Cumbria Partnership

Daniel Hallan, Head of Digital Technology NHS England (North) Greater Manchester Health & Social Care Partnership, Healthier Lancashire & South Cumbria

Royal Holloway University of London (RHUL)

Prof. Keith Mayes introduced the work of the Information Security Group at Royal Holloway.

He then defined ransomware – malicious software that gains access to your computer system. Typically it can render the stored data inaccessible to the user, or prevent the computer from functioning normally. One attack is to encrypt the user's data with a key known only to the attacker, then present the user with a pop-up screen demanding payment in Bitcoin for the data to be decrypted/restored.

Prof. Mayes advised that one should never pay the ransom, as it encourages the attacker's business case. One also needs to be aware that sometimes malicious software (malware) claims to be ransomware, but is permanently destructive and so it may not be possible to restore the data after

payment. Even in the case of data being restored after a ransom is paid, there is always a lingering doubt as to what else was put onto your machine?

How does in the malicious software get into a system?

For large scale infection we are mainly concerned about remote access via the Internet, but we should not forget about local physical devices, such as USB sticks, CD Rom, DVD or mobile phone. Wannacry was initially blamed on an employee clicking on an email attachment, which is a known and generic means of infection, but this was not to blame in this case. There was a vulnerability in a Windows protocol implementation so the ransomware could enter the system infecting almost everything as it passed through.

How can you defend yourself?

A sensible precaution is to try and educate users to spot strange emails; however with so many emails and users, there is always likely to be someone who will click on a malicious attachment. There are studies to show how people judge if an email is genuine or fake, however attackers will also be following this research and so genuine emails may become more difficult to tell apart from the fake ones. Training will help, but it does not eliminate the problem.

Systems and software should be kept patched and up to date to reduce the likelihood of becoming a victim of ransomware. Patching usually involves installing a small software update on a computer, to repair a known fault or security vulnerability. It is important to remember that patches fix known problems not unknown ones. It is generally a good idea to do patching, but the Petya ransomware came about through this mechanism. In this case, rather than infecting the victim's machines directly, the attackers infected the suppliers of an accountancy software package. The malware was then distributed to the customer-base in the guise of software patches

What can you do when an attack happens?

Many firms have disaster recovery plans, but they may not be suitable for ransomware attacks. Regular backups are good practice, but you need to be careful about how they are managed. We know that if you are a targeted organisation the attackers can play a long game, and could perhaps spend a year infecting your systems before the attack starts. You may have been backing up the infected software without knowing it and overwritten older "clean" backups Furthermore, some backups involve copying data to a local server or to cloud storage, but if these are accessible as network drives, they may also be visible to the attackers and hence at risk of encryption and ransom.

Are there any developments that may help?

Machine learning experts around the world are trying to detect infection by looking at software behaviours.

Dr Daniele Sgandurra explained that Wannacry exploited zero day vulnerabilities. A zero-day vulnerability is a flaw which hackers can use to exploit a PC or computer system, as it is unknown to existing security protection or patching systems. RHUL is looking at how ransomware behaves and how it is different (abnormal) from legitimate software. We can then look for common features that occur in ransomware products to assist early detection.

Comments from the floor

1. A lot of companies are investing in anti-virus software, so we need to learn who to trust. For emails, check that the style is correct. Ask if the email address is correct? Look out for small

spelling differences that betray the attacker. In a human way we look for small differences, machine learning is similar.
2. If the supply chain is compromised, then it is hard to get to grips with the ransomware.

What do we as politicians need to know, how can we help?

1. Boards need to understand the risks that they face. Surprised that hospital boards were surprised when they were hit as they ran with outdated systems for a long time. It is about corporate risk management
2. The Computer Misuse Act – keen to see this reviewed such that it gives greater cover. Some simple amendments would help UK plc to defend itself against attacks.

   We are not asking for offensive action, e,g, a "hack back". We need a better definition of what information can be taken from a command and control server that belongs to or is under the control of an offending party? Even to look at it would be an offence under the Computer Misuse Act.

3. CMA is comprehensive but prosecutions are very limited. These prosecutions are often against good people trying to work through a problem and falling foul of the law. More about where you draw the line, the guidance is important.

NHS North

What happened on the 12th May?

Declan Hadley – was responsible overall for response. First made aware around 10.00 a.m. Lancashire and South Cumbria cover 5 acute hospitals, one County Council and two local authorities. Around 5000 machines infected. Primarily effected desktops and not clinical machines. Business continuity plans were implemented immediately. It helped that the attack was on a Friday afternoon as fewer patients were around. Many medical staff continued to use infected machines.

Took ten days to completely restore the estate which covers a number of machines and many were managed by 3rd party contractors. Huge support from Council colleagues and NHS England and NHS Digital.

Key learning points:

1) Many aspects were avoidable. Applying patches means many 100s of systems and roll-out takes time. People were updating software but it takes time.
2) Better control of external contractors.
3) Integrated network across health and social care in Lancashire and South Cumbria. This means more organisations are involved. This is not universal across the NHS.
4) Remedial action was thorough and well done. Lots of collective work, many clinical staff are peripatetic. How do we get security levels up?

Have we learnt enough, will it happen again on Friday?

No, attacks continually mutate so you can put a lot of actions in place but all sorts of things can go wrong. The nature of the next attack is probably different and they happen every day. The human factor is the most crucial and the NHS has many phishing attacks.

NHS is looking at the 4th generation collaborative network and cyber security is at the heart of this. Wannacry was a watershed moment for the NHS. It changed the perception of digital IT in the NHS as a whole from being a basement level activity to an activity that is everyone's challenge. This is a positive in that it has opened peoples' eyes.

Nationally , had conversations about support from other colleagues. Access to knowledge and expertise such as GCHQ would be good.

Workstations were hit but not the server estates. Very few workstations had data saved on them. No patient data was lost at all across the whole of the system. The primary responsibility was to get things up and running.

XP – Vast majority of the estate was not XP, mostly Windows 7, 8 or 10. MRI scanners are the exception as they have XP embedded. The original patch from MS did not actually work . The system globally was not prepared for this.

XP story was a red herring.

Patch did not work for a number of reasons. Each locality rolled out the patch differently and Declan has 5 under his control. Do not know why it did not work. Update software is pushed out centrally and different machines would report different reasons for not updating. This was in March. MS has many different versions of Windows and users have many different versions of their PC build. It could also be a network glitch.

Centrally these problems were known and the response was to send out staff to individual machines. Machines would need to be prioritised so typically servers with patient data get remedial action first. MS released a single standalone patch on 12th May which worked.

Comments from the floor

1. Lots of different hardware and patches so each one has to be tackled and fixed. Need more standardised versions of OS. A targeted patch only tries to update one thing. People do not want to patch all the time so applying patches in a timely manner is a problem.
2. Petya and Wannacry scrapped credentials out of the memory and using normal log-on processes. How many of the 9000 were effected by credential stealing?. Lancashire took a belt and braces approach, wiped everything to stop the attack.
3. Everyone knows that these attacks happen, a home PC will have as many as 5 per day.
4. Lancashire and South Cumbria covers 110,000 staff on Active Directory because they have an integrated system which makes it a weakness. Larger scale networks are being built as social and healthcare integrate more.
5. Is the NHS more at risk than other organisations and was the UK more vulnerable? What can Parliamentarians take away?

   There are valuable elements from the national IT programme such as nationwide licencing agreements. No more vulnerable than anywhere else. Integration is what is happening and will increase as we merge social and healthcare systems. Not particularly about investment.

   NHS is becoming more integrated and these large systems are a risk. IT tends to report into Finance so decisions are made at a financial not Board level. IT needs to come out from under someone else and be a direct Board report.

6. Is Governance changing? Yes but it is recognised. Trusts that were not hit though might not take this governance issue quite so seriously.
7. What is the role of NHS Digital? NHS England is the commission, Digital is a provider of national systems. They have been key in providing support but are focussed on national programmes.
8. Who grips the issue of governance? NHS England.
9. Are they getting to grips with governance? A report is due soon from William Smart on this topic. There is a high degree of scrutiny across NHS North. There is a lot of governance, safer than May but not a guarantee that this will not happen again. Cyber security is much higher on Board agendas.
10. One lesson to be drawn is that of the provider and the user. In the Armed Forces the defence companies go to war with the soldiers. Is the relationship better between the NHS and suppliers?
11. Layered security, what is the NHS doing? Perimeter security was reasonably robust, intrusion detection systems also. Multiple points of response on intrusion detection. MS is used to scan the network. Will be appointing a regional security officer to help co-ordinate them.
12. Wannacry source attribution has not been made but is likely to be a nation state.