theguardian

NHS seeks to recover from global cyber-attack as security concerns resurface

Cybersecurity centre says teams ‘working round the clock’ to fix systems rendered inaccessible by international ransomware attack

Damien Gayle, Alexandra Topping, Ian Sample, Sarah Marsh and Vikram Dodd

Saturday 13 May 2017 09.16 BST

The NHS is working to bring its systems back online after it became the highest-profile victim of a global ransomware attack and faced renewed concern about the strength of its infrastructure.

The National Cyber Security Centre (NCSC) said teams were “working round the clock” in response to the attack, which resulted in operations being cancelled, ambulances being diverted and documents such as patient records made unavailable in England and Scotland.

Computers at hospitals and GPs surgeries in the UK were among tens of thousands hit in almost 100 countries by malware that appeared to be using technology stolen from the National Security Agency in the US. It blocks access to any files on a PC until a ransom is paid.

The British prime minister, Theresa May, and NHS Digital said they were not aware of any evidence patient records had been compromised in Friday’s attack, which is thought to have affected computers in nearly 100 countries.

May said: “This is not targeted at the NHS, it’s an international attack and a number of countries and organisations have been affected.”

Amber Rudd, the home secretary, refused to confirm on Saturday morning whether patient data had been backed up, and said the NHS would upgrade its software in the wake of the attack. She said data “should” be backed up, but would not say whether it actually had been.

The shadow health secretary, Jonathan Ashworth, urged the government to be “clear about what’s happened”, describing the attack as “terrible news and a real worry for patients”.

The unprecedented attacks, using software called WanaCrypt0r 2.0 or WannaCry, exploits a vulnerability in Windows. Microsoft released a patch - a software update that fixes the problem - for the flaw in March, but computers that had not installed the security update were vulnerable.

In December it was reported that nearly all NHS trusts were using an obsolete version of Windows for which Microsoft had stopped providing security updates in April 2014. Data acquired by software firm Citrix under freedom of information laws suggested 90% of trusts were using Windows XP, then a 15-year-old system.

It is not known how many computers across the NHS today are still using Windows XP or recent variants Windows 8 and Windows 10.

About 40 NHS organisations are though to have been affected by Friday's bug, which was released the day after a doctor warned that NHS hospitals needed to be prepared for an incident precisely of the kind seen.

In an article published in the British Medical Journal, Dr Krishna Chinthapalli, a neurology registrar at the National Hospital for Neurology and Neurosurgery in London, said hospitals "will almost certainly be shut down by ransomware this year".

Ross Anderson, of Cambridge University, said the "critical" software patch released earlier this year may not have been installed across NHS computers. "If large numbers of NHS organisations failed to act on a critical notice from Microsoft two months ago, then whose fault is that?" Anderson said.

Alan Woodward, a visiting professor of computing at the University of Surrey, said the attack's success was "likely to be because some organisations have either not applied the patch released by Microsoft, or they are using outdated operating systems."

NHS Digital said on Friday night it was unable to comment on the suggestion.

Marco Cover, a systems security researcher, said critics should take into account the complexity of keeping systems up to date. "It's easy to blame people who don't upgrade," he said. "But in practice things are often more complicated: operations teams may not touch legacy systems for a number of reasons. In some cases they may even be unaware that such legacy systems are running in their infrastructure."

The same malicious software that hit NHS networks attacked some of the largest companies in Spain and Portugal, including phone company Telefónica, and has also been detected on computers in Russia, Ukraine and Taiwan among other countries. The international shipping company FedEx was also affected.

Kaspersky Lab, a cybersecurity company based in Moscow, estimated that 45,000 attacks had been carried out in 99 countries, mostly in Russia. In a blogpost, it added that the totals could be "much, much higher".

In the UK, computers in hospitals and GP surgeries simultaneously received a pop-up message demanding a ransom in exchange for access to the PCs.

A warning was circulated on Friday within at least one NHS trust of "a serious ransomware threat currently in circulation throughout the NHS", but the attack proved impossible to stop. Patient records, appointment schedules, internal phone lines and emails were rendered inaccessible and connections between computers and medical equipment were brought down. Staff were forced to turn to pen and paper and to use their own mobile phones.

Last year the government established the NCSC to spearhead the country's defences. In the three months after the centre was launched, there were 188 "high-level" attacks as well as countless lower-level incidents. The chancellor, Philip Hammond, disclosed in February that the NCSC had blocked 34,550 potential attacks targeting UK government departments and members of the public in six months.

The Patients Association condemned the criminals behind Friday's attack, and said lessons from earlier incidents had not been learned. "It has long been known that the NHS struggles with IT in multiple respects and that this includes serious security problems," it said.

Infected computers show a message demanding a $300 (£233) ransom per machine to be paid to a Bitcoin wallet address. It says: "Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

"You only have three days to submit the payment. After that the price will be doubled. Also if you don't pay in seven days, you won't be able to recover your files forever."

NHS Digital confirmed that a "number of NHS organisations" had been affected and refused to confirm or deny reports that put the total as high as 40. "The investigation is at an early stage but we believe the malware variant is Wanna Decryptor," it said. "At this stage, we do not have any evidence that patient data has been accessed. We will continue to work with affected organisations to confirm this.

"NHS Digital is working closely with the National Cyber Security Centre, the Department of Health and NHS England to support affected organisations and to recommend appropriate mitigations."

British law enforcement agencies said they believed the attack was criminal in nature, as opposed to a cyber-attack by a foreign power, and was being treated as serious but without national security implications.

One NHS worker, who asked to remain anonymous, said the attack began at about 12.30pm and appeared to have been the result of phishing. "The computers were affected after someone opened an email attachment. We get a lot of spam and it looks like something was sent to all the trusts in the country. Other hospitals have now been warned not to open these emails - all trusts communicate with each other."

Another NHS worker, who works at an Essex hospital and also asked to remain anonymous, said her team's computers went down at about 2pm. "We were told to shut down, take out network cables and unplug the phones," she said. "A message came up for just one of our team about the fact that all the files would be wiped in two hours unless we gave $300 in bitcoins."

Dr Chris Mimnagh, a GP in Liverpool, said his surgery had "severed links" to the wider NHS network as a precaution. He said: "Unable to access our clinical system - as a precaution our area has severed links to the wider NHS, which means no access to our national systems, no computers means no records, no prescriptions, no results. We are dealing with urgent problems only. Our patients are being very understanding so far."

Lorina Nash, 46, from Hertfordshire, was bringing her mother for an appointment at Lister hospital in Stevenage when systems went down. "We have been here since 12.30pm and the computers were affected at about 12pm - patients are still waiting around but most of the A&E patients have been sent to other hospitals. I have never seen accident and emergency so empty.

"They gave my mum a blood test but have had to send her blood to Cambridge by courier for testing. They said it could take two or three hours before it comes back with a result."

Dr Asif Munaf, a gastroenterologist at Chesterfield hospital, said there was a backlog of patients in its A&E, which he said had been badly affected because it was unable to book new patients on the system.

“From my ward’s point of view, we’re not able to make referrals to, for example, psychiatry because they use a different system to us,” he said. “Everything’s getting delayed. Patients who were supposed to go home this afternoon won’t go home until Monday because they now won’t be seen and get a follow-up plan. It’s quite unfortunate for the patients.”

Dr Christopher Richardson, the head of the cybersecurity unit at Bournemouth University, said the process of recovering the NHS’s IT systems would involve a painful and longwinded “deep strip” of affected computers.

“You go down to the basic machine, you take everything off it, you reconfigure it and then you build it back up again,” he said. “If you’re talking national health, you’re talking a lot of machines on a single site and you’ve got to get them all because these nasty pieces of malware, they float around, so they only have to remain on one machine and when you reboot it will deliver the same thing again.”

Additional reporting by Sam Jones in Madrid

Topics

Hospitals

NHS, Health, Cybercrime, news