BTS SIO - Internet security

A - Compréhension orale :

1- Watch the following video on Youtube: https://youtu.be/-ni_PWxrsNo

2- Préparez un compte-rendu oral de la vidéo : donnez le maximum d'informations que vous comprenez.

B – Compréhension écrite :

Health to be on cyber-security's front line in 2021

Gordon Corera, Security correspondent, BBC News, published28 December 2020

Covid-19 catapulted the health sector to the forefront of cyber-security in 2020, but the next year is likely to see the dangers continue and evolve. Threats from nation states and criminals to the health system are a growing concern. The huge logistical challenge of rolling out vaccines faces the risk of disruption to complex supply chains. And criminal ransomware poses a threat at a time when the pandemic has increased our reliance on technology.

Supply chain

The distribution of the various coronavirus vaccines may bring relief, but it also brings with it a major challenge: many of those involved have not had to think hard about security in the past.

The complex global supply chain for vaccines ranges from factories in one country to internet-connected fridges in another. It will create new pressure on doctors' surgeries, IT systems, and sometimes small providers who play a critical role. IBM has already said it has seen suspected state-hackers target the "cold chain" used to keep supplies at the right temperature during transportation. And in the UK, the National Cyber Security Centre, which worked quickly when the pandemic began to secure vaccine research, has since pivoted its efforts towards vaccine distribution.

At least the large pharmaceutical companies are no stranger to cyber-espionage. Their security officials say they first began thinking hard about the issue after a major espionage campaign back in Spring 2010. But the issues around the pandemic have changed the sector's importance.

"We are now on a grander stage," is how one person involved puts it.

In July, the UK accused Russian intelligence of targeting research, including for the Oxford vaccine, while the US accused Chinese hackers of similar activity. The emergence of "vaccine nationalism" led intelligence and security officials to raise questions about whether countries could try and undermine the efforts of others going forward.

"It could be trying to steal the intellectual property for financial purposes," Tonya Ugoretz of the FBI told a recent Aspen Institute Cyber Summit. "It could be to undermine confidence... or to advantage another country's own development.

"We see our most determined nation-state adversaries not just relying on one method to target the supply chain, but combining cyber with using more traditional espionage and human sources."

One much discussed tactic is the deliberate spread of misinformation online about vaccinations, or questioning a country's safety and testing record. The UK Army's 77th Brigade has supported a Cabinet Office investigation into whether foreign states are driving anti-vaccine fears within the UK. Most sentiment was domestically generated, head of Strategic Command General Sir Patrick Sanders said at a recent Chatham House event. And he raised the possibility of retaliation.

"Where these things are being fuelled from overseas, then we will take action, and if the NCF (National Cyber Force) has a part to play in that, it will."

Cyber-blackmail campaigns

But despite concerns about states, experts say, criminal ransomware - the locking of people out of their computers and data until they pay - remains the more serious and persistent threat. There was some talk at the start of pandemic from criminal gangs that they would not target health. But it did not last and attacks have multiplied. A recent report from security firm Positive Technologies says half of all the cyber-attacks on healthcare were ransomware in the July-to-September quarter of 2020.

US hospitals have been worse hit than the UK. It is thought this is because criminals see them as richer than their NHS counterparts. In just 24 hours in October, six American hospitals received ransom demands of at least $1m (£810,000), leading to some cancer treatments being cancelled.

"The healthcare sector has become such a big, rich, juicy target," Greg Garcia, executive director for the US Cybersecurity of the Health Sector Co-ordinating Council, recently said. "It's as if they moved on from the financial services sector."

The UK has made stride to fix weaknesses in the NHS systems exposed by 2017's Wannacry ransomware attack. Even so, there are concerns it could be hit again. Dr Saif Abed has long warned that such an attack could kill a patient. He is a former NHS doctor who left clinical practice to set up the AbedGraham group, which advises on IT security risks to health.

"The thing that's really concerning is that attackers now understand the concept of clinical urgency," he says. "They understand: 'If we create a risk that disrupts the ability to provide patient care, we're more likely to get a payout.'"

His worry is that the pandemic has accelerated the digitisation of health. While that has brought benefits such as consultations taking place online, he says the investment needed to keep internet-connected systems and devices secure has not kept pace. Dr Abed says he often hears security researchers talk about hacking insulin pumps to kill someone. But he says a bigger risk is the fact that more devices are being connected together while remaining vulnerable, leading to the risk of a cascade effect.

He adds that his biggest worry is that criminals move from just locking organisations out of their health data to starting to tamper with it, posing risks to patient safety. The desire to limit further Covid-19 outbreaks may also create a further drive to share data more broadly. And that in turn may present further opportunities to steal or subvert it.

Another sign that the cyber-security of health is likely to be on the front line in 2021.

Questions

a) Which sector will be mostly targeted by cyber-criminals in 2021?

b) True or false? Justify with a quote from the text.

- The distribution of COVID-19 vaccine is hacker-proof.

- Pharmaceutical companies are used to be hacked.

- Hackers may be working for foreign countries to steal information.

- One of the hackers' tactics is to spread disinformation.

c) What is the most serious hacking threat?

d) Were hospitals attacked by hackers?

e) Explain, in your own words, the concept of "digitalization of health" (line 54).