HealthManagement.org
Promoting Management and Leadership

Boost to England's health cyber security following £150 investment

£150 million will be spent on NHS cyber security over the next three years¸ reducing the impact of an attack, announced the Department of Health and Social Care.

The department has announced a new multi-million pound Microsoft security package that will ensure all health and care organisations can use the most up-to-date software with the latest security settings.

Under the new security plan, NHS Digital will have near real-time capability to respond to cyber-attacks. Systems will have increased resilience to attacks, and unsupported Microsoft systems in the NHS will be a thing of the past.

Cyber attacks are a real and growing threat to healthcare organisations, and they have become a top priority for the UK Government. On May 12, 2017, the WannaCry cyber-attack affected a wide range of countries and sectors, including at least 80 out of 236 NHS trusts and a further 603 primary care and other organisations, including 595 out of 7,454 general practices.

Since 2017, the Government has invested £60 million to address key cyber security weaknesses. Organisations across the industry have commended the increased investment for the next three years, which will enable NHS Trusts to benefit from enhanced security intelligence.

Sarah Wilkinson, Chief Executive at NHS Digital said: “We welcome the Secretary of State’s commitment to prioritise cyber security. The new Windows Operating System has a range of advanced security and identity protection features that will help us to keep NHS systems and data safe from attack. This is one of a suite of measures we are deploying to protect the service from cyber attack.”

Windows Defender Advanced Threat Protection will feed into a central NHS Security Operations Centre, creating a centralised, managed, and coordinated framework for the detection of malicious cyber activity and visibility around how threats try to move across the organisation. The service will use Microsoft's vast telemetry sets, advanced analytics, and expert human analysts to reduce the likelihood and impact of security breaches or malware infection.

At a local level, individual trusts will have the ability to detect threats, isolate infected machines and kill malicious processes before they are able to spread.

Another area of investment includes £21 million on upgrading firewalls and network infrastructure at major trauma centre hospitals and ambulance trusts. The aim is to improve security at key emergency sites and protect technology such as MRI scanners and that used for blood test analysis.

The Department has launched a Data Security and Protection Toolkit which requires health and care organisations to meet 10 key standards, including appointing a senior executive to oversee data and cyber security. Meanwhile, new powers have been given to the Care Quality Commission to inspect NHS trusts on their cyber and data security capabilities in conjunction with NHS Digital.

£39 million has been spent this year by NHS trusts to help them address infrastructure weaknesses which prevented them from fully implementing solutions to address all historic cyber alerts.

Health Secretary Jeremy Hunt said: “We know cyber attacks are a growing threat, so it is vital our health and care organisations have secure systems which patients trust.

“We have been building the capability of NHS systems over a number of years, but there is always more to do to future-proof our NHS against this threat.

“This new technology will ensure the NHS can use the latest and most resilient software available – something the public rightly expect.”

Cyber security across all organisations is a top priority for the UK Government, which is why it is investing £1.9 billion in the National Cyber Security Strategy and opened the National Cyber Security Centre (NCSC), which manages around 60 serious attacks every month.

Improved resilience to attacks achieved through the new plan will help to protect the NHS system and patients within it. The UK’s Royal Academy of Engineers has warned that hackers could kill patients by attacking their wearable health monitors, such as pacemakers and heart pumps.

Wearable health monitors that are linked to the internet or internal computer networks could provide a gateway for hackers to plant ransomware into systems, which threatens victims if ransoms aren't paid.

Professor Nick Jennings, a fellow of the Royal Academy of Engineers and Vice Provost at Imperial CollegeLondon said: “We cannot totally avoid failures or attacks, but we can design systems that are highly resilient and will recover quickly.” With cyber threats increasing, investments in security will need to keep up with hacker innovation.

Published on : Wed, 9 May 2018