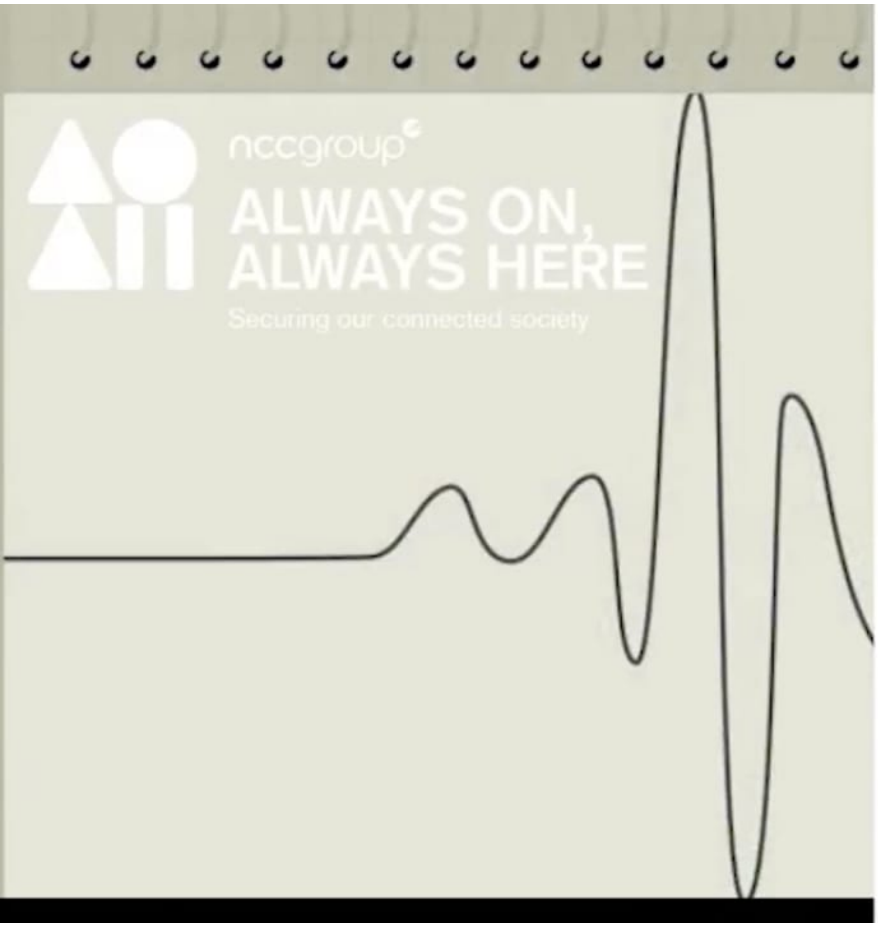

SECURITY SURGERY
WITH
MATT LEWIS

ANSWERS TO YOUR MOST
FREQUENTLY ASKED QUESTIONS
ON CONNECTED HEALTH

Jul 17, 2020 16:14 BST

Security Surgery with Matt Lewis Part Three: Connected Health

As part of our Always On, Always Here campaign, which explores how we make our connected society safer and more secure, we're answering some key questions about cyber security in smart cities, everyday routines, connected health and more.

In this four-part series, Matt Lewis, Research Director, provides the answers and explains how the work we do shapes and secures our society in ways that you might not be aware of.

In this edition, we're focusing on connected health, from typical threats to the

impact of COVID-19 and our work to make the sector safer and more secure. Watch the video or read the Q&A below and get in touch if you want to find out more.

View embedded content here

What are the typical threats to the connected health industry?

Fundamentally, we've seen that where there are very flat networks and infrastructures across healthcare organisations, these can exploited by attacks like the Wannacry ransomware attack on the NHS, which spread pervasively quite quickly.

In connected health, ransomware outbreaks could impact the ability to deliver critical healthcare provision or impact on life support devices, so the threat goes beyond compromised networks and data privacy and becomes a matter of life and death. It's likely that we'll continue to witness these kinds of attacks in the health sector.

Threats to data privacy are also a big concern for the industry. Most health-related data is personal and sensitive in one way or another, so the protection of that data, the individuals that have access to it and knowledge of why it might be being used in certain applications all need to be considered.

There's a lot to consider. Even at the technical level, threat actors can actively target device manufacturers to impact on the availability of their

products. If successful, these attacks could have significant health-rated consequences and even result in loss of life in a worst-case scenario.

We regularly blog about threats to connected health and have recently published a few whitepapers on this topic, so if you'd like to learn more, please check out the content at the bottom of this page, or visit our newsroom.nccgroup.com for more information.

How has COVID-19 impacted the risk profile of the NHS and other healthcare providers?

We've seen many threat actors using COVID-19 as a theme to legitimise their phishing and social engineering campaigns. There is a heightened sense of fear and uncertainty at the moment, so if a campaign is sufficiently convincing around the topic of COVID-19, it could trick people into clicking on links or downloading things that they wouldn't act on under normal circumstances.

We've also seen more reports of hospitals being hit by ransomware attacks. There's definitely been a continuation, if not a rise, in these types of attacks against healthcare providers. We also anticipate an increase in advanced persistent threat (APT)-type entities targeting the healthcare sector during this period. Most countries around the world are desperately looking for new types of drugs and are experimenting with different types of care, and there's a lot of intellectual property and sensitivity around that data. One can imagine that there are APT actors actively seeking to try and get hold of that data, just as they are trying to get hold of sensitive data in other critical sectors like banking and telecoms.

What is NCC Group doing to make connected health safer and more secure?

As with smart cities, we are working, researching and engaged at many different levels. For example, we are working with connected health device manufacturers to help them understand how they can improve the secure development lifecycle of their products, from hardware component specifications to the code that goes into those devices.

We are also helping them to ensure that those components are as effective as they can be when it comes to minimising disruption or resisting possible

remote attacks when they are connected to health networks.

We're also supporting a number of hospitals and health authorities to help them understand everything from how they can ensure secure network architecture and design on their hospitals, and how they can isolate particularly sensitive devices and systems.

Finally, we're studying emerging protocols in the connected health space, and providing our input in terms of what security features should be built into those protocols, both at the design stage and implementation.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750