Media Release

Ransomware Attack a Wake-Up Call

Tuesday 17 May 2018 – The WannaCry ransomware attack that has impacted an estimated 300,000 users in 150 countries is a wake-up call for both government and business, said the global body for ICT professionals.

Mike Hinchey, President of IFIP (International Federation for Information Processing), today warned that WannaCry was only the latest in a series of online attacks that are likely to escalate in coming weeks and months.

“While we don’t yet know who is responsible for the WannaCry attacks, we do know that the ransomware was developed out of exploits leaked or stolen earlier this year from America’s National Security Agency (NSA), which had been stockpiling them for use in surveillance,” said Mr Hinchey.

“This is the first widespread application of those exploits, but it’s only a matter of time before other attempts are made using adapted versions of the surveillance tools taken from the NSA.”

ICT Professionals Must Maintain Standards

Mr Hinchey said ICT professionals must take responsibility for ensuring that systems within their domain are up to date and protected from external threats like ransomware or spyware.

“People responsible for procuring, implementing and maintaining ICT systems have a duty of care to ensure that critical infrastructure and data are protected. In our increasingly connected world, where computers run everything from utilities and transport platform to banking systems and even life support facilities in hospitals,” he said.

“Government agencies and companies seeking to save money by delaying software upgrades need to consider the potential cost of leaving key systems undefended against cyber attacks is much higher than simply losing access to some information.”

The WannaCry attacks were focused on older versions of the Windows operating system (OS) which are no longer automatically supported by Microsoft. However, in environments such as Britain’s National Health Service (NHS), which still uses Windows XP to maintain compatibility with internal business systems, the ICT professionals managing these systems should purchase security updates from Microsoft to ensure that their critical infrastructure is protected.

Mr Hinchey said the biggest impacts are being felt in organisations with outdated software like NHS and in countries like China and Russia, where many people use pirated software that doesn’t receive regular vendor updates.

Moreover, procurement processes for new systems that seek only to leverage ICT to make or save money often fail to consider issues relating to technology and security maintenance which are integral and thus contractable requirements for services, software and devices. This short-sighted approach can create situations where security and other maintenance become extremely expensive. In our increasingly connected world where more devices and systems are connected via the Internet of Things (IoT), this risk will only grow.

“Cybercrime is not new. The ICT profession has processes and standards in place to protect users from external attacks, but if these processes have not been followed then users and systems are left vulnerable,” Mr Hinchey said.

IFIP Duty of Care for Everything Digital

Last November, IFIP’s professionalism arm, IP3, launched iDOCED, the IFIP Duty of Care for Everything Digital Initiative. iDOCED is designed to remind and support both providers and consumers of digital products and services that they have a duty of care in ensuring that they act responsibly in relation to the digital world.

At the time, IP3 Chair, Brenda Aynsley said, “The iDOCED seeks to raise awareness of what users can and should do to protect themselves in today’s digitally-connected world, and to highlight the need for companies to act responsibly and ethically in the development and implementation of commercial products and services.”
IFIP wants companies to ensure their products and services HIT the mark for their clients, customers and the broader community, where HIT stands for Honour, Integrity and Trust, all of which are part of the Duty of Care for ICT professionals in the execution of their work.

In relation to ransomware attacks, IFIP recommends that users implement regular backups of all important files and ensure that they are using up to date software with automated updates installed. “Microsoft released a patch back in March for the vulnerability being exploited by the WannaCry ransomware, but the update must be applied in order for it to be effective,” said Mr Hinchey.

“If there was a fault in our cars (software or otherwise) that caused a big issue, even potentially death, we’d expect the manufacturers to do a recall. Why are ICT companies more lax? Surely they must take greater responsibility?” he queried.

ENDS

For more information about ICT security, contact IFIP or your national ICT professional body, which can be identified by visiting the IFIP website at where its 50 member societies are listed.

ABOUT IFIP

IFIP, the International Federation for Information Processing, is the global professional federation of societies and associations for people working in Information and Communications Technologies and Sciences. Established under the auspices of UNESCO in 1960 and recognised by the United Nations, IFIP represents ICT professional associations from more than 50 countries and regions with a total membership of over half a million. It also brings together more than 3,500 scientists from industry and academia, organising them into over 100 Working Groups and 13 Technical Committees to conduct research, develop standards and promote information sharing. Based in Austria, IFIP organises and supports over 100 conferences each year, fostering the distribution of research and knowledge to academics and industry practitioners alike.

Website: http://ifip.org
Latest news: http://ifipnews.org
Twitter: http://twitter.com/ifipnews
LinkedIn: https://www.linkedin.com/company/ifip---international-federation-for-information-processing

Media contacts
Caroline@quantumvalues.com
Shuba@quantumvalues.com