20th October 2021

2N STRENGTHENS CYBERSECURITY GUIDANCE FOLLOWING LATEST RESEARCH ON CYBER CRIME

- *Hiscox's Cyber Readiness Report 2021 revealed that the cyber threat to businesses is increasing, with access control an area of vulnerability for many companies*
- *During European Cybersecurity Month 2020, 2N published guidance for companies to help them prevent cyber attacks; 12 months on, the guidance has been strengthened in response to the growing threats levels*

To mark European Cybersecurity Month 2021, 2N, the global leader in IP access control systems, has strengthened its guidance to help consumers and building managers prevent cyber attacks. The move is a response to evidence that the threat of cyber crime is increasing, and that access control remains a common area of vulnerability.

Earlier this year, Hiscox published its Cyber Readiness Report 2021. It was based on a survey of more than 6,000 companies based in the US, the UK, Spain, the Netherlands, Germany, France, Belgium and Ireland. The report confirmed that spending per business on cybersecurity has more than doubled in the last two years as a direct response to growing threat levels. Almost half of the respondents said that they felt their organisation had become more vulnerable to cyber attacks since the start of the pandemic, rising to 59% among businesses with more than 250 employees. 28% of the businesses surveyed who had suffered attacks were targeted on more than five occasions last year. One in six of the companies that had been victims of cyber crime said that a cyber event threatened the viability of their business.

Hiscox went on to assess firms' maturity across six different areas which comprise the elements required to install, run, manage and govern an effective security system. One of those six areas was 'Identity and access management', and, across all the companies surveyed, it came second bottom of the list.

In response to these findings, 2N has strengthened its guidance to help consumers and building managers prevent cyber attacks which were first published during European Cybersecurity Month 2020. Two new pieces of advice have been added:

1. **Pursue compliance with a proven security control framework.** Two of the most respected are ISO 27001 and SOC 2. These guide companies in creating secure systems and processes.

2. **Make sure the access control system includes the use of encryption and multi-step authentication.** This protects communication between devices, controllers and mobile devices, and ensures no back doors for ‘maintenance purposes’.

Tomáš Vystavěl, 2N's Chief Product Officer, said: “We felt that it was necessary to strengthen our cybersecurity guidance partly because the threat is increasing, but also because many companies are still playing ‘catch up’ when it comes to cybersecurity in access control. This matters because if the access control system is compromised, the daily operation of the building – and, consequently, its residents – is immediately at risk. Attitudes are changing, but they need to change even faster.”

2N’s full list of advice for preventing cyber attacks is provided below.

For more details about 2N’s approach to cybersecurity: https://www.2n.cz/en_GB/about-2n/cybersecurity

2N’S GUIDANCE FOR PREVENTING CYBER ATTACKS

1. **Pursue compliance with a proven security control framework.** Two of the most respected are ISO 27001 and SOC 2. These guide companies in creating secure systems and processes.

2. **Make sure the access control system includes the use of encryption and multi-step authentication.** This protects communication between devices, controllers and mobile devices, and ensures no back doors for ‘maintenance purposes’.

3. **Create an independent network, dedicated exclusively to devices that handle sensitive information and ensure that communication between them is encrypted.** Place these devices to a separated virtual LAN (VLAN) and ensure that manufacturers of installed devices or software use implementation protocols such as HTTPS, TLS, SIPS or SRTP by default.

4. **Create different accounts with different privileges.** Doing this ensures that users will only be able to make changes related to their specific tasks, while the administrator will be given greater privileges to manage the building and all linked accounts.

5. **Update the software regularly.** Installing the latest firmware version on devices is important to mitigate cybersecurity risks. Each new release fixes bugs found on the software by implementing the latest security patches.

6. **Train your employees to avoid social engineering threats.** The human element is the most vulnerable part of any system, and attackers can trick people into making security mistakes or giving away sensitive information. It is therefore necessary to train employees regularly and invest in their awareness of cybersecurity.

About 2N

2N is the global leader in IP access control systems.

2N has been in the vanguard of innovation in the sector, developing the world's first IP intercom in 2008 and the first LTE/4G intercom ten years later. The company's portfolio includes door phones, answering products and access control systems. 2N specialises in the residential sector and has products which are Bluetooth-, smartphone- and tablet-enabled.

2N takes design just as seriously as innovation – and has the Red Dot and iF Design Awards to prove it.

2N was founded in 1991 in the Czech Republic. Prague remains the global headquarters, with teams now in eight other countries (USA, United Kingdom, Germany, Italy, France, Spain, UAE and Australia) and an extensive distribution network throughout the rest of the world.

For more information, visit www.2N.com