Five things an employer needs to instil in remote teams to halt the rise of ransomware

Ransomware UP by over 200% in the first half of 2021 – what can an employer do to advise staff?*

ProLion, a best-in-class proactive ransomware and data protection solution for ONTAP storage, has today issued five top tips for employers looking to secure their organsiations from ransomware attacks as a direct result of insider threats or plain negligence.

Ransomware is on the rise globally targeting industry and organisations with a number of high profile attacks already this year. It is without doubt creating a number of significant cybersecurity challenges.

Robert Graf, Founder, ProLion, stated: “Ransomware is a type of malware where key files are encrypted by hackers that then renders data inaccessible to the victim. To put it bluntly it is criminal extortion which sees hackers promising to restore systems and data when ransom is paid by the victim.

“But with many employees still working remotely, many organisations are struggling with breaches as a direct result of poor security management. This can and does open the door to an insider threat – either through negligence or malicious intent. As a result we have developed a Five Point Plan for HR and risk and compliance teams which, if implemented throughout a distrpubted enterprise, will lead to reduced risk of attack.”

1. Don’t store proprietory data on personal laptops: this makes any remote worker a highly attractive target in the first place. This risk has increased dramatically as a result of people working from home as a result of the pandemic. And while efforts have been made with the roll-out of new security levels, if your employee still stores data on their hard drive, not a lot will stop the hackers and while this is plain negligence, businesses must also regnise the issue of insider threats

2. Be sensible with your digital profiles: employers must begin to take a stronger line on employees who continually post where they work and what they do. Guidance needs to be issued to all employees on what can and cannot be posted on social media in relation to their jobs. No-one is suggesting pulling off social media platforms altogether, just being more circumspect on what information is posted.
3. A word about passwords: It goes without saying that a password must be a tough as possible and not the same one across all employee accounts. It should also be stressed to employees that when they are prompted for a change in a password, they do just that – change it and not just reuse the old one.
4. Browsing: there are plenty of security tools out there that block access to certain sites if you are working on a company laptop. But if an employee is using their own you may have less control. The message for employers and emplyees alike is to get educated on the very real possibility that you could end up with a malware infection as a direct result of visiting a dodgy site.
5. Don't engage in online conversations with people you do not know: we all know the risks associated with catfishing. Your personal data or your employers data is a highly attractive target for many.

Graf concluded: "Today's distributed business and IT environment, whn seen in conjunction with the inter-connectivity of digital commerce, means an expanded attack surface for bad faith actors. Like the bank robbers of old, cybercriminals go where the money is accessible, and the easier it is the easier for them to reap benefits from extortion.

"It only takes one click by an employee to infect an entire network, spreading from a local computer to Network Attached Storage. That is where our solution sits, detecting and blocking attacks aiming to access propriatory data.

"For the distributed organisation the challenge is to protect and defend the enterprise across a far greater estate. Now is the time for business leaders, risk and compliance experts, IT departments and HR to work in tandem to reduce that exposure and call time on the hackers."

Notes to editors

About ProLion

ProLion GmbH is a developer of ransomware protection and data integrity software solutions for any ONTAP focused storage environment and high-availability solutions for SAP and MetroCluster environments.

Founded in Austria, ProLion's best-of-breed CryptoSpike solution eliminates system downtime and data loss risk ensures that an organisations' data remains secure, compliant, manageable, and accessible.

www.prolion.com

* Analysis from NCC Group's Research Intelligence and Fusion Team (RIFT)