EngineerIT

Electronics, computer, information & communications technology in engineering

2017
june

FEATURING

Automation & control

Measurement & instrumentation

Electronics

Telecommunications

Computing & software

FLUKE. by comtest
Fluke 729
Automatic Pressure Calibrator.
Generates accurate pressure
for single or multiple tests.

ISSN 1991-5047

Wannacry, the board and the IT department

by Prof. Basie van Solms, University of Johannesburg

Prof. Basie von Solms

The month of May brought with it the biggest cyberattack in the history of computers – the Wannacry ransomware attacks. The real impact of the attacks will probably never be known, but maybe the clinical statistics of the attacks are not the most important consequences to investigate. There can be no doubt that this is not a standalone event, and that we will see more and more such attacks in in the future – so what are the real lessons we can and should learn from these attacks so that we can be better prepared for the next one?

Again, there are many aspects of these attacks that can be studied, such as the role of the National Security Agency (NSA), the role of Microsoft, speculation on who started it and more. However, that will not necessarily help us to better prepare for the next one.

It is clear that the attacks were successful on those computers and IT systems where basic information and cyber security best practices were missing – practices like ensuring regular and continuous application of updates and patches, ensuring proper and regular comprehensive backups of data and information, ensuring good security awareness amongst users to not fall for social engineered attacks. These are basic practices which were in existence long before the internet was even operational. Victims who suffered from the attacks can blame NSA, Microsoft, the cybercriminals and everybody else, but not checking your own security practices and policies can have serious consequences.

Furthermore, it also became clear that many victims still used older versions of the relevant operating systems, like Windows XP, which is not supported any more in terms of updates, patching etc. I see this as negligence on the part of the relevant company, and by continuing to do so, users are simply inviting the next attack. I realise that replacing (upgrading) something like XP is not easy because it is embedded in many endpoint types of systems and will be costly. However, that is no excuse as the risk is too big – and as far as I am concerned, this is not a decision to be made on the technical level – it is a corporate governance issue. If the company board is made aware of such risks and does not take the lead in addressing this, then we must expect more class actions against companies, and specific board members; by clients, customers and more. Too often role players like the IT department and IT manager or even the CIO are seen as the guilty parties by senior management in such an attack. It is the responsibility of such role players to clearly convey the risks of such outdated systems, practices and implementations to the board and executive management. The board must accept the risk, and the consequences, if it is decided not to provide the financial sources to eliminate such risks. Cyber security governance is a board responsibility and accountability, and cannot be transferred to anybody else. There may well be some future court cases resulting from board members being held personally accountable for negligence in this area.

So, what is the message of Wannacry?

Firstly, the concept of cyber security governance as board and executive management accountability must be ingrained in the structure of any company, and must be understood and acted upon accordingly. Cyber security governance must become a permanent point on the board's agenda. Secondly, international best practices in information and cyber security governance must be endorsed by the board and executive management and enforced by the IT department. If these lessons are not learnt from the Wannacry attack, prepare yourself for the next one!

Send your comments to engineerit@ee.co.za