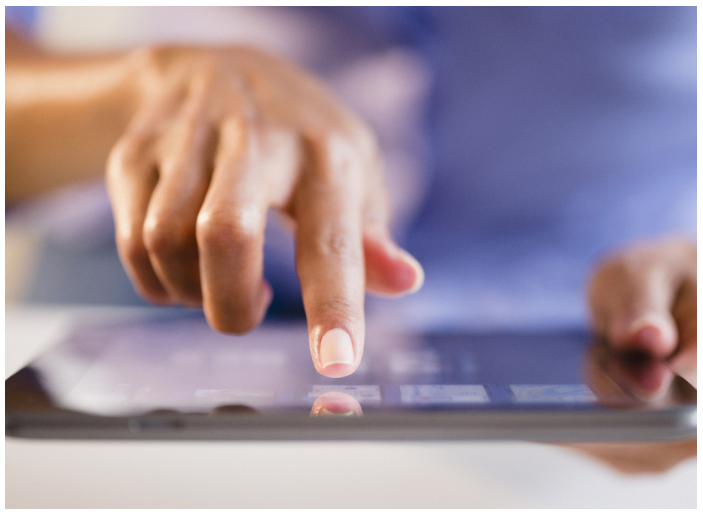
Protecting yourself and your organisation from ransomware

There was a time in Nigeria when kidnapping was the order of the day. Recently we have heard of high profile kidnappings where the abductors would take innocent people and demand a ransom from their family members and loved ones before they are released. It may interest you to know that cyber criminals have designed mechanisms whereby they can also "kidnap" your critical information and demand for a ransom to get it released.

Ransomware are software used by attackers to encrypt, or lock your information, making it unreadable and unusable. The attackers would demand for a ransom to be paid before they can release such information. It is a criminal business model that has proven extremely profitable as some of the advanced actors stand to make millions of dollars from the 'trade'. What makes it very effective is the lack of a backup system which raises the chances that the victim would consider paying the ransom.

Ransomware have been in existence for several years but according to an article released by the FBI in April 2016, there has been a sharp increase in the number and variants of ransomware affecting organizations around the world, moreso in Nigeria between 2015 and 2016. Some of the common variants include: CryptoLocker, 73v3n, Locky, Jigsaw, Samsam, Rokku, KeRanger, Cerber and WannaCry ransomware that hit individuals and organizations in about 100 countries on 12 May 2017.

The experience of a ransomware lockdown can be frightening. A bank would not be able to provide services if all the information about its customers and transactions are no longer available. It would not have access to information about their account transactions or information to correctly identify them. The whole production line of a manufacturing /energy company may grind to a halt if the core systems are exposed to a ransomware attack. Other processes (e.g. inventory, supply chain) would also be adversely affected. If the core system of the central switch (i.e. for electronic transactions)



of Nigeria is encrypted, e-commerce would be adversely impacted and this would affect businesses and individuals across the country. These are just some of the areas in which ransomware can cripple organisations, individuals and even a nation. Anyone is a potential victim.

Unlike what many people think, the mode of attack for ransomware is as simple as being infected by a computer virus (which is also a malicious software installed on users computer/device to perform the attackers bidding). Ransomware can infect victims through any of the following means:

- Clicking on links in phishing emails
- Opening documents in phishing emails
- Clicking on erroneous links on infected websites
- Downloading unlicensed software

The ransomware would be saved on the victim's computer/device and encrypt documents in a format that cannot be read by any computer, while propagating itself to other computers within the network. In most cases, the infected systems may display more information about the ransomware and instructions on how the victim should make payment.

Even though the mode of attack for ransomware is a lot like the conventional computer virus, protecting oneself/ organization from ransomware is very different from that of a virus. Protection from a virus may involve using an antivirus software and keeping it updated however, this approach may not be effective for a ransomware. This is because a lot of antivirus work by comparing the signature (pattern) of all files on your system with a large database of known virus signatures.

Therefore, if a file with an unknown signature attacks your system, there is very little chance that the antivirus would detect it or clean it. Some ransomware may even encrypt or modify their own source code therefore making it harder for antivirus software to detect it.

What then can we do to protect ourselves and organizations from ransomware? Some of the methods discussed below can be employed:

Examine emails and understand the context: Do not click on email links or open files embedded emails especially when you do not know the sender or are not familiar with the context of the email. For example, if you suddenly receive an invoice/receipt from a sender you do not know, or have never done business with, then you should verify the sender before opening the document. In addition, macros (self-executable MS Office documents) from Microsoft Office files transmitted over email, should be disabled.

Employ safe internet browsing techniques: When browsing on the internet, ensure you visit genuine websites and avoid clicking links in pop-up boxes. Use common sense and a healthy dose of skepticism when browsing on the internet.

Perform effective security awareness: Organizations should embark on effective cyber security awareness campaigns to educate personnel about ransomware and the precautions they should take to be protected.

Use heuristic/behavioral antivirus: Move away from the traditional antivirus model of comparing signatures, to a model that understands the normal workings of your computer and notices when something abnormal occurs (e.g. sudden encryption of files).

Regularly update software: Use the latest versions of application software. This can provide an added layer of protection against online threats as some ransomware are deployed via vulnerability exploits (i.e. flaws in outdated applications).

Always maintain a recent back-up of your data: The simplest way to recover from a ransomware attack is to restore your documents and files from a backup. However, many organisations and individuals do not maintain recent backups of all their files and folders so this may not be as simple as it sounds. Backups should be comprehensive, have integrity and be recent enough to be useful.

Maintain visibility of your network: Recent attacks have demonstrated that ransomware-style attacks are as the last phase of a multifaceted attack strategy. The encryption of data can be used as a distraction to prevent an organization from uncovering other activities of the attacker. It may be used to cover the tracks of the attacker trying to escape with information, delete data or implant malware tools to be used in the future. With this in mind, it would be possible to see the telltale signs before the encryption of information finally takes place. Some of the signs may include, users executing programs with elevated privileges, deactivation of Windows firewall or antivirus system and download of a malicious file on a system. These can only be detected if the organization maintains vigilance regarding the activities on all systems within its network.

Devise efficient response techniques: The saying goes that you can only prepare for war in the time of peace, therefore the best time to prepare for a ransomware incident is when it has not yet occured. Organizations need to segment their information assets and also put a price tag on each of them, this would help define their risk appetite and decide the next course of action when a ransomware attack happens (i.e. how to recover).

Business Continuity/Disaster recovery plans should include simulations for ransomware attacks which are tested regularly so that every stakeholder is clear on actions to be taken. Employees responsible should be trained on how to effectively detect and contain these types of attacks.

As doctors say, prevention is better than cure, therefore it is imperative that organizations and individuals take the security of their systems and critical information very seriously because with the "click of a button" this information can be captured or even rendered non-existent.

Contact

Anthony Olukoju
Partner and Leader
Risk Advisory Services
aolukoju@deloitte.com.ng

Tope Aladenusi
Partner
Risk Advisory Services
taladenusi@deloitte.com.ng

Funmi Odumuboni
Manager
Risk Advisory Services
fodumuboni@deloitte.com.ng