Thinix®

Network Security After Facing A Cyberattack

How To Secure Your Network

White Paper

How do I know my network is secure after a ransomware event or known intrusion?

Answering this question is pretty difficult because hackers can install backdoor applications which can lie dormant for any amount of time, exposing themselves only at specific times/dates, or which can lie dormant and can be triggered by a change in an external website or DNS. Other forms of backdoors can modify the firmware on hardware devices such as your hard drive[1], flash drives, network cards, routers, switches, wireless access points or printers. Even other forms of malware can install at the kernel level and can make modifications to the operating system, making themselves undetectable[2].

Because there are thousands of attack vectors, confirming with confidence that the network is secure can be extremely difficult. A network once breached by hackers runs a large risk of still being unsafe even after the original threat has been remedied.

Taken a step further, hacker's aren't nice people. Chances are if they have taken your money once, they will try to do it again, and even if you've paid them to get your data back, you cannot assume that they will not retain a backdoor access to your network.

We can run significant numbers of tests, trying to prove the network is secure, but it is impossible to prove a negative, which is the fundamental point of this article. A network threat that lies dormant is somewhat difficult to understand but is an important point which should drive the decisions we make to guard our data and protect our networks.

You cannot prove a negative[7]

There is a fundamental difference between science and mathematics in that mathematics allows for 'proof' of theories, where science is based on observations, repeatability applied to the scientific method.

With this in mind, we can come to a fundamental paradigm which is: 'You cannot prove a negative.'

To understand this, we will use an example of a doctor with a patient who wants to know with certainty that they do not have cancer.

The patient goes to the doctor who performs every scientific test possible today on the patient. After a barrage of tests, the doctor still cannot tell the patient "you do not have cancer" because a patient may have cancer but the cancer isn't observable using any of the scientific methods used by the doctor for a diagnosis. Instead, the doctor must say; "We have performed all the tests we have the ability to perform, and all the tests came back with no positive results for cancer." To elaborate further, our ability to prove something is limited by the tests we know how to perform, and if the tests don't discover something we are looking for, the result may be an incorrect assumption.

In the book *The Black Swan Theory*, the concept of exhaustive testing and inconclusive results is discussed in detail. The book is named after the paradigm that even after millions of white swans have been observed, that it doesn't prove that all swans are white. When the first black swan is observed, it came to change the scientific perspective overnight, and the observance of only a single black swan came to dispel a lifetime of evidence that until observed, indicated that all swans were white.

Computer infections are exactly like this; antivirus companies may scan for viruses and not detect anything, even when the system is completely owned by a hacker.

Is my network secure after a ransomware or known intrusion?

In the same context, we are often asked: "Is my computer, or network compromised?" When we are asked this question, it is important for us to answer just like the doctor above. We cannot say unequivocally that the computer or network is not compromised, we can only perform all the tests we know how to perform, and if these tests turn up no evidence of hackers, we can then say that the results of our testing indicate that it has not been compromised (hackers appear to be out). This is somewhat confusing to people because they think that computer software should be more like mathematics than science. The issue is that hackers can utilize thousands of different techniques to infect things, and in doing so, these things can be outside our realm of observation[2].

Why replace hardware after ransomware or known intrusion?

Taken a step further, if it were highly probable that a hacker had penetrated a network, where the computers were outdated, it might be logical to simply replace the workstations altogether. If the systems were not replaced, the company would risk spending hundreds or thousands just to reformat the outdated systems only to arrive at the conclusion that the systems still might not be 100% clean. After a known security compromise, even after spending hundreds or thousands of dollars in testing, it is difficult to provide an adequate level of insurance that devices have not been compromised. Stated in yet another way, the level of risk imposed by not being positive that a hacker is not present is nearly impossible to tell, and companies who tell you otherwise may be making dangerous assumptions.

One example of this is software which exploits hard drives[1]. Within a hard disk, there is a disk controller, which is a chip that keeps track of bad sectors on the hard drive. When a bad area is detected by the disk controller, the bad area is removed from the usable space which is presented to the operating system.

When this occurs, this disk space still exists on the disk, but the contents of that disk area are no longer visible to the operating system. When this occurs, theoretically a virus could exist in these bad sectors, and it would not be perceivable to the operating system.

When hackers replace the firmware on the disk controller, they can do exactly this. Through special commands, the hackers can map out areas on the disk, and the operating system can no longer read these areas. By using special commands to their special firmware, hackers can still write to and read from these bad sectors.

When this occurs, a naïve computer person may look at a computer and could run every antivirus program in existence, and the virus could not be detected. Only by understanding that this is a possibility could someone examine the drive controller firmware, to determine if it is a bit-for-bit, checksum accurate version.
To combat these specific problems, vendors such as Hewlett-Packard (HP) have invented technologies[3] that allow them to digitally sign the firmware on hardware devices, and allow that software to be validated by running a special software application. The problem is that these technologies are only supported on some hardware, and they are not present on all hardware. HP calls their technology Sure Start, and they have begun incorporating this into various products including high-end workstations, printers, and digitally signed hard drives for servers.

Beware Of Rootkits

Rootkits allow third parties remote access to a PC, and are typically used by IT professionals for remote fixes or troubleshooting network issues[1]. However, rootkits can become nefarious once installed on your computer; rootkits allow attackers to hijack your computer, steal data, or install other pieces of malware. Rootkits are designed to go unnoticed and actively hide their presence[1]. Only with manual monitoring are experts able to detect this type of unusual malicious behavior. Regular patches to the operating system and software are also required to eliminate potential infection routes[1].

Note[1] – Kaspersky Lab, "Computer Viruses and Malware Facts & FAQs"

So what do you do after a ransomware or network intrusion?

The answer to this question depends on who you are. For example, the remediation requirements for a bank would be different (and more strict because millions of dollars are at stake) than for a very small business. However, in general, you need a competent networking company to examine all the hardware, workstations and servers. Other steps include but are not limited to:

- Changing all network passwords
- Verifying that network equipment doesn't use default passwords
- Implementing file monitoring software on all file servers
- Implementing business-class firewalls with:
  - Stateful packet inspection
  - Proxies for common traffic
  - WatchGuard Threat Detection & Response (TDR)
  - Offsite or protected logging
  - Reporting so that you can notice abnormal traffic
- Examining log files from onboard diagnostics such as HP Insight Manager or Dell iDRAC
- Examining log files from all workstations and servers
- Implementing a comprehensive antivirus solution with a single dashboard
- Network monitoring systems to establish baseline monitoring
- Reformatting or replacing affected workstations, servers and other infected hardware
- Verifying firmware software images on printers, routers, switches, etc.
- Implement good backup policies and have a professional audit your backup strategy
- Identify all data on the network and implement a policy of least permissions to reduce the number of employees who have access to critical data.
- Implement secure networking policies (beyond the scope of this document), but these policies will prevent users from having the ability to install software, restrict domain administrator access to workstations and eliminate file sharing.
- Consider implementing layer-2 network isolation (PVLAN's)
- Segment networks to minimize exposure and compartmentalize damage
- Consider dedicated use workstations for high-security operations such as SCADA, or online banking.
- Consider implementing other intrusion detection systems

By implementing a comprehensive, layered approach networks can be protected as best as possible. Thinix has multiple network security solutions that can help you. Call us at (888) 484-4649 or email sales@thinix.com to boost your network security.

Thinix Managed Security Services Package

Detect & Protect Against Today's Most Advanced Security Threats!

AssuredSecurity™

For Secure PCs:
Endpoint & detection management

321-Backup®

For Secure Data:
Secure offsite data backup

Threat Detection & Response

For Secure Networks:
Managed network security

References:

1. NSA / Equation Group malware infects hard drive firmware:
   http://bit.ly/2pRoLQj
   http://bit.ly/2tiQOxV

2. DoublePulsar runs in kernel mode to evade detection:
   https://en.wikipedia.org/wiki/DoublePulsar
   http://bit.ly/2tiPw63

3. HP Sure Start - Automatic Firmware Intrusion Detection and Repair System: http://hp.care/2tPbx8w

4. New security features in HP's printers can detect rogue BIOS and firmware modifications: http://bit.ly/2tP8Ow7

5. Protecting embedded systems from unauthorized software modifications: http://bit.ly/2rSD2BS

6. Bug in Dell BIOS makes systems vulnerable to attacks:
   http://bit.ly/2sRPjp9

7. Evidence of Absence - "A lack of proof is not proof of lack"
   https://en.wikipedia.org/wiki/Evidence_of_absence

8. James Randi Lecture - Can't prove a negative:
   https://www.youtube.com/watch?v=qWJTUAezxAI

9. Micron SSD Security Firmware Features Technical Brief: https://www.micron.com/~/media/documents/products/technical-marketing-brief/ssd_security_firmware_features_tech_brief.pdf

10. Sophisticated, Undetectable DoublePulsar Attack Used Against Hardened Defenses: http://nyti.ms/2tyfJKJ