



Global Knowledge®

Expert Reference Series of White Papers

13 Infrastructure Decisions That Result In Poor IT Security

13 Infrastructure Decisions That Result In Poor IT Security

James Michael Stewart, Global Knowledge Instructor, CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+, Security Windows 2000, MCSA Windows Sever 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, iNet+

Introduction

Designing, architecting, and implementing a corporate network is a daunting task. It is easy to become lost in the minutia and overlook some big picture issues. This is especially true in regards to security. Some decisions that make sense in terms of efficiency, throughput, compatibility, ease of administration, etc., might not result in good security. This white paper presents 13 somewhat common infrastructure decisions that can result in poor IT security. (They are not in any particular order.)

1. Choosing Speed over Security

A high-performance network that supports efficient productivity is highly desirable. However, when a decision must be made between a reduction in throughput versus increased security, security should be valued at least as highly as productivity. Without security, productivity will not last. Without proper and sufficient security controls, malicious code or hacker attacks can quickly render a network infrastructure unable to support legitimate communications or transactions. High-speed communications are important, but we must protect the availability of the network in order to have a network.

2. Implementing a Single Internet Connection

Any single point of failure is a poor infrastructure and design decision. There should be two exits from every room. There should be at least two copies of every file. And there should be at least two connection paths out to the Internet. (There is an assumption here that Internet connectivity is an essential utility of the organization. If not, then redundancy is not as important.) With only a single connection to the Internet, there is a single point of failure. One mis-configured connection device, one hardware failure, one payment lost in the mail, one misguided backhoe, and the connectivity is lost. Every aspect of a network should be designed with redundancy in mind in order to avoid single points of failure.

3. Failing to Implement Internal Traffic Management

More than half of security breaches are caused by internal personnel. It is often incorrect to assume all users, programs, and processes within the organization's network are safe and trustworthy. Every moderate to large network should implement traffic shaping, traffic throttling, and traffic control measures internally. By implementing these features, no one network service, application, protocol, or user can fully consume all of the network bandwidth to the exclusion of others. Thus, mission-critical communications will always have sufficient bandwidth reserved for them.

4. Not Using Network Event Auditing

Evidence of compromise is a valuable asset. However, it can only be obtained at the instant the compromise is performed. If the network is not already actively recording network events into a log file or audit trail, then security breaches will go unnoticed. It is better to record events to a log file that are not needed, than to not record events that are essential to detection, response, and potential prosecution. Without an ongoing permanent record of events (i.e., log files), you have no evidence of benign or malicious activity, and trends toward bottlenecks will go unnoticed as well.

5. Depending on Physical Security

Every environment must properly address logical/ technical security, administrative security (i.e., policies and people), as well as physical security. Each of these three areas is somewhat self-contained in that the security measures of one do not ensure protection against threats from the other. In other words, logical protections defend against logical attacks, and physical security defends against physical attacks. It is a mistake to assume a strong physical security solution is compensation for poor or lax logical security. Malicious code and social engineering attacks are still possible even with an impenetrable physical fortress. Just as with logical security, there are a wide variety of physical security options. You need to implement those that are relevant to your specific needs. However, some common examples of physical security controls include security cameras, security guards, lighting, conventional and electronic locks, burglar alarms, man traps, fencing, fire resistant building materials, and fire detection and suppression systems.

6. Assuming the Electrical Service Is Reliable and Consistent

Electricity is the life blood of computer technology. Without power, computers and networks fail. And not just any power; pure, consistent, clean, regulated power is necessary for the long-term viability and stability of computer networks. Power grids can and do fail. The power company cannot guarantee uninterrupted service or prevent electrical noise. You must use surge protectors, power line conditioners, uninterruptible power supplies, and on site power generators to ensure only consistent, conditioned power is fed to your electronics. The loss of power, even for short periods of time, means operational downtime and potentially lost or corrupted data.

7. Failing to Store Backups Offsite

Bad things happen. You must be prepared. Backups are the only form of insurance against data loss. Without backups, your data is at risk. Serious risk. Real risk. You need to follow the backup 3-2-1 rule:

- There must be 3 copies of data
- There must be 2 different forms of media
- There must be 1 copy stored offsite

Failing to store a backup offsite is also a failure of taking the real world seriously. Complete and total destruction by fire, flood, tornado, and other acts of nature is common. No home or office building is completely protected. Assume the worst, and then plan to survive it. No, not just survive, but thrive through it. Be better prepared than your neighbors or competition. Be the first to fully recover and be back in business.

8. Leaving Unused Ports Open

Leaving unused ports open and active is the same as leaving your back door unlocked while you go on vacation. Anyone can connect an unauthorized system to an open port. System hardening has two basic steps: remove what you don't need, lock down what is left. If a physical port is not in use, disconnect it, turn it off, make it go dark. When you need the port in the future, then re-enabled it. Don't enable any connection path before it is secured or before it is needed for a business task.

9. Deploying Wireless Networks

Wireless networks are a challenge to secure and support. Often, the cost in effort as well as budget is not worth it when compared to using a physical cable. Before deploying a wireless network, ask a few questions.

1. Will a power cord be needed anyway? If so, running a network cable as well will not be much additional effort.
2. Is the wireless for customers or visitors? If so, it does not need any link into the private LAN; a public ISP link would suffice.
3. Are any essential business tasks dependant on wireless? If not, you might not be implementing wireless for a real business reason.

I would generally recommend against installing wireless networks for most organizations. This is because interference and DoS are always possible, even with the best wireless security configured and the strongest wireless encryption enabled.

10. Not Planning for Mission-Critical Task Interruptions or Disasters

Murphy (as in Murphy's Law) hates you. The universe tends towards entropy. The only thing that remains the same is change. Assuming your organization will continue to function into the future exactly the way it does now is a fantasy. Things will change; some for the good, many for the bad. Natural disasters, malicious code, fire, thieves, disgruntled employees, criminal hackers, and the rambunctious children of your employees can cause mission-critical task interruptions, downtime, and disasters. By failing to plan, you plan to fail. You must plan your response and recovery now before a business interruption occurs. Disaster recovery planning focuses your recovery on the most mission-critical processes in priority over less essential functions.

11. Avoiding Hardware Replacements Based on MTTF/MTBF

The most common cause of unplanned downtime is hardware failure. Most devices are tested and rated based on how long they should operate under normal conditions before experiencing their first failure. This is a time rating of either mean time to failure (MTTF) or mean time before failure (MTBF). MTTF is for devices that are

usually replaced upon failure. MTBF is for devices that can be repaired and returned to service. The MTBF thus serves as the measure for the time frame before the first failure and between all subsequent failures. Hardware should be scheduled for replacement/repair around 95% of its MTTF/MTBF. While some statistical outliers will fail earlier, and some might last for much longer without failure, statistically, the odds are in your favor when you plan to replace devices just before their average failure time is reached.

12. Allowing Outside Portable Media

Any communication pathway that supports legitimate transmission of data can also be used to transfer malicious code. One of the more notorious culprits of this is removable media. Whether CD, DVD, floppy, zip disk, smart card, flash drive, or USB hard drive, all of them present a real and current risk. Many forms of malicious code can spread through removable media one machine at a time. If a system is infected, potentially any storage device connected to that machine can become infected. Then as that storage device is connected to other computers, the malicious code spreads. When anyone brings removable media in from anywhere there is a significant risk of infecting the company network. Make it company policy that all media from outside sources must be screened and scanned on a dedicated malware scanning system before being used on any other office computer.

13. Allowing End Users to Install Software

Another common method of distribution of malicious code is the Trojan horse, which is a supposedly benign program that happens to contain a hidden malicious payload. When the host program is used, the malware is delivered. Trojan horses can be obtained from removable media brought in from outside sources, downloaded from the Internet, exchanged through peer-to-peer services, received as an e-mail attachment, and shared across network services. When regular users have sufficient permissions to install new software, they, in turn, also have permission to launch malicious code. One method to eliminate this risk (or at least significantly reduce it) is to prevent end users from being able to install software. One way to accomplish this is through the use of a white list. A white list is a file of the names and hash values of all executables that the organization has deemed safe and necessary for users to accomplish their work tasks. Only the applications on the white list will execute on the user's system. All other programs, including any installation process or malware, will fail to execute as it will not have permissions to do so. White listing does restrict a user's freedom, but on a work computer, security is often more important than granting users complete control over their workstations.

Summary

I hope your organization is not making all of these mistakes in its infrastructure decisions. It is possible that your organization can improve its security in one or more of these areas. Take the time to assess your current security policy in each of these areas to see if there is room for refinement or improvement. Keep in mind that security is never an accomplishable goal. Instead, it is a long and difficult journey that requires vigilance and persistence in striving towards improved security over time.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

[Security+ Prep Course](#)

[Understanding Networking Fundamentals](#)

[CISSP Prep Course](#)

For more information or to register, visit www.globalknowledge.com or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and Onsite sessions, to meet your IT and business training needs.

About the Author

James Michael Stewart has been working with computers and technology for over 25 years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, CEH, and Security+. He is the primary author on the *CISSP Study Guide 4th Edition* and the *Security+ 2008 Review Guide*. Michael has also contributed to many other CISSP- and Security+-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware.

In addition, Michael has co-authored numerous books on other security and Microsoft certification, and administration topics. He has developed certification courseware and training materials, and has presented these materials in the classroom. Michael holds the following certifications: CISSP; ISSAP; SSCP; MCT; CEI; CEH; TICSA; CIW SA; Security+; MCSE+; Security Windows 2000; MCSA Windows Sever 2003; MCDST; MCSE NT & W2K; MCP+I; Network+; and iNet+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants, hands-on, "street smarts" experience. You can reach Michael by e-mail at michael@impactonline.com.