"Highest Performance
Lowest Price"

Microsoft GOLD CERTIFIED Partner

GFI WHITE PAPER

SECURITY THREATS: A GUIDE FOR SMALL AND MEDIUM BUSINESSES

What does an SMB need?

A successful business works on the basis of revenue growth and loss prevention. Small and medium-sized businesses are particularly hit hard when either one or both of these business requirements suffer. Data leakage, down-time and reputation loss can easily turn away new and existing customers if such situations are not handled appropriately and quickly. This may, in turn, impact on the company's bottom line and ultimately profit margins. A computer virus outbreak or a network breach can cost a business thousands of dollars. In some cases, it may even lead to legal liability and lawsuits.

The truth is that many organizations would like to have a secure IT environment but very often this need comes into conflict with other priorities. Firms often find the task of keeping the business functions aligned with the security process highly challenging. When economic circumstances look dire, it is easy to turn security into a checklist item that keeps being pushed back. However the reality is that, in such situations, security should be a primary issue. The likelihood of threats affecting your business will probably increase and the impact can be more detrimental if it tarnishes your reputation.

This paper aims to help small and medium-sized businesses focus on threats that are likely to have an impact on, and affect, the organization. These threats specifically target small and medium-sized business rather than enterprise companies or home users.

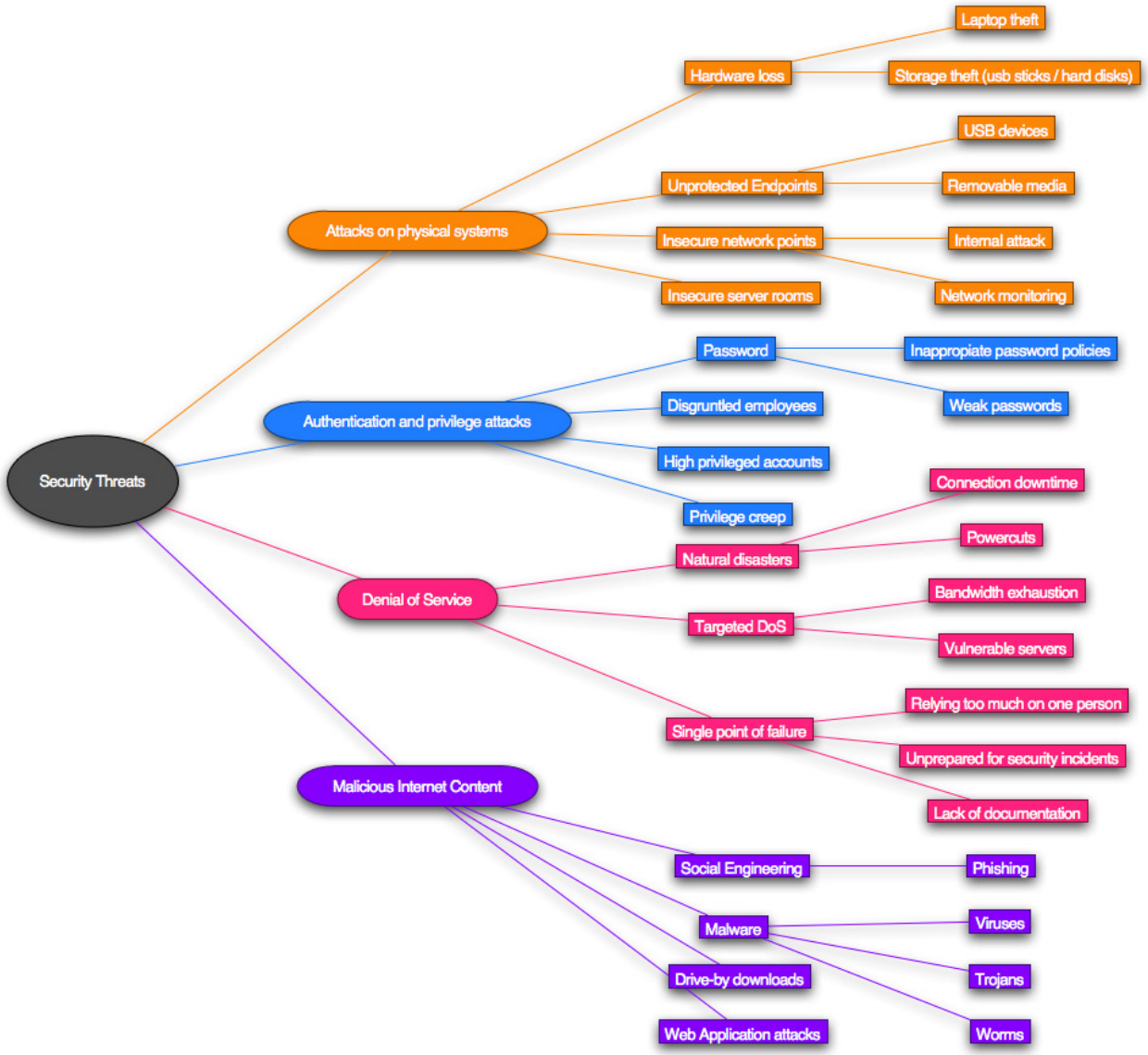

Figure 1. Security threat map

Security threats that affect SMBs

Malicious Internet Content

Most modern small or medium-sized businesses need an Internet connection to operate. If you remove this means of communication, many areas of the organization will not be able to function properly or else they may be forced to revert to old, inefficient systems. Just think how important email has become and that for many organizations this is the primary means of communication. Even phone communications are changing shape with Voice over IP becoming a standard in many organizations.

At some point, most organizations have been the victim of a computer virus attack. While many may have anti-virus protection, it is not unusual for an organization of more than 10 employees to use email or the internet without any form of protection. Even large organizations are not spared. Recently, three hospitals in London

had to shut down their entire network due to an infection of a version of a worm called Mytob. Most of the time we do not hear of small or medium-sized businesses becoming victims of such infections because it is not in their interest to publicize these incidents. Many small or medium-sized business networks cannot afford to employ prevention mechanisms such as network segregation. These factors simply make it easier for a worm to spread throughout an organization.

Malware is a term that includes computer viruses, worms, Trojans and any other kinds of malicious software. Employees and end users within an organization may unknowingly introduce malware on the network when they run malicious executable code (EXE files). Sometimes they might receive an email with an attached worm or download spyware when visiting a malicious website. Alternatively, to get work done, employees may decide to install pirated software for which they do not have a license. This software tends to have more code than advertised and is a common method used by malware writers to infect the end user's computers. An organization that operates efficiently usually has established ways to share files and content across the organization. These methods can also be abused by worms to further infect computer systems on the network.

Computer malware does not have to be introduced manually or consciously. Basic software packages installed on desktop computers such as Internet Explorer, Firefox, Adobe Acrobat Reader or Flash have their fair share of security vulnerabilities. These security weaknesses are actively exploited by malware writers to automatically infect victim's computers. Such attacks are known as drive-by downloads because the user does not have knowledge of malicious files being downloaded onto his or her computer. In 2007 Google issued an alert [1] describing 450,000 web pages that can install malware without the user's consent.

Then you get social engineering attacks. This term refers to a set of techniques whereby attackers make the most of weaknesses in human nature rather than flaws within the technology. A phishing attack is a type of social engineering attack that is normally opportunistic and targets a subset of society. A phishing email message will typically look very familiar to the end users – it will make use of genuine logos and other visuals (from a well-known bank, for example) and will, for all intents and purposes, appear to be the genuine thing. When the end user follows the instructions in the email, he or she is directed to reveal sensitive or private information such as passwords, pin codes and credit card numbers.

Employees and desktop computers are not the only target in an organization. Most small or medium-sized companies need to make use of servers for email, customer relationship management and file sharing. These servers tend to hold critical information that can easily become a target of an attack. Additionally, the move towards web applications has introduced a large number of new security vulnerabilities that are actively exploited by attackers to gain access to these web applications. If these services are compromised there is a high risk that sensitive information can be leaked and used by cyber-criminals to commit fraud.

Attacks on physical systems

Internet-borne attacks are not the only security issue that organizations face. Laptops and mobiles are entrusted with the most sensitive of information about the organization. These devices, whether they are company property or personally owned, often contain company documents and are used to log on to the company network. More often than not, these mobile devices are also used during conferences and travel, thus running the risk of physical theft. The number of laptops and mobile devices stolen per year is ever on the increase. Attrition.org had over 400 articles in 2008[2] related to high profile data loss, many of which involved

[1] http://news.bbc.co.uk/2/hi/technology/6645895.stm

[2] http://www.attrition.org/dataloss/

stolen laptops and missing disks. If it happens to major hospitals and governments that have established rules on handling such situations, why should it not happen to smaller businesses?

Another threat affecting physical security is that of unprotected endpoints. USB ports and DVD drives can both be used to leak data and introduce malware on the network. A USB stick that is mainly used for work and may contain sensitive documents, becomes a security risk if it is taken home and left lying around and other members of the family use it on their home PC. While the employee may understand the sensitive nature of the information stored on the USB stick, the rest of the family will probably not. They may copy files back and forth without considering the implications. This is typically a case of negligence but it can also be the work of a targeted attack, where internal employees can take large amounts of information out of the company.

Small and medium-sized businesses may overlook the importance of securing the physical network and server room to prevent unauthorized persons from gaining access. Open network points and unprotected server rooms can allow disgruntled employees and visitors to connect to the network and launch attacks such as ARP spoofing to capture network traffic with no encryption and steal passwords and content.

Authentication and privilege attacks

Passwords remain the number one vulnerability in many systems. It is not an easy task to have a secure system whereby people are required to choose a unique password that others cannot guess but is still easy for them to remember. Nowadays most people have at least five other passwords to remember, and the password used for company business should not be the same one used for webmail accounts, site memberships and so on. High profile intrusions such as the one on Twitter[3] (the password was happiness), clearly show that passwords are often the most common and universal security weakness and attacks exploiting this weakness do not require a lot of technical knowledge.

Password policies can go a long way to mitigate the risk, but if the password policy is too strict people will find ways and means to get around it. They will write the password on sticky notes, share them with their colleagues or simply find a keyboard pattern (1q2w3e4r5t) that is easy to remember but also easy to guess. Most complex password policies can be easily rendered useless by non-technological means.

In small and medium-sized businesses, systems administrators are often found to be doing the work of the network operators and project managers as well as security analysts. Therefore a disgruntled systems administrator will be a major security problem due to the amount of responsibility (and access rights) that he or she holds. With full access privileges, a systems administrator may plan a logic bomb, backdoor accounts or leak sensitive company information that may greatly affect the stability and reputation of the organization. Additionally, in many cases the systems administrator is the person who sets the passwords for important services or servers. When he or she leaves the organization, these passwords may not be changed (especially if not documented) thus leaving a backdoor for the ex-employee. A startup company called JournalSpace[4] was caught with no backups when their former system administrator decided to wipe out the main database. This proved to be disastrous for the company which ended up asking users to retrieve their content from Google's cache.

The company's management team may also have administrative privileges on their personal computers or laptops. The reasons vary but they may want to be able to install new software or simply to have more control

[3] http://tinyurl.com/bysvuf
[4] http://tinyurl.com/6ulyqs

of their machines. The problem with this scenario is that one compromised machine is all that an attacker needs to target an organization. The firm itself does not need to be specifically picked out but may simply become a victim of an attack aimed at a particular vulnerable software package.

Even when user accounts on the network are supposed to have reduced privileges, there may be times where privilege creep occurs. For example, a manager that hands over an old project to another manager may retain the old privileges for years even after the handover! When his or her account is compromised, the intruder also gains access to the old project.

Employees with mobile devices and laptop computers can pose a significant risk when they make use of unsecured wireless networks whilst attending a conference or during their stay at a hotel. In many cases, inadequate or no encryption is used and anyone 'in between' can view and modify the network traffic. This can be the start of an intrusion leading to compromised company accounts and networks.

Denial of Service

In an attempt to minimize costs, or simply through negligence, most small and some medium-sized businesses have various single points of failures. Denial of service is an attack that prevents legitimate users from making use of a service and it can be very hard to prevent. The means to carry out a DoS attack and the motives may vary, but it typically leads to downtime and legitimate customers losing confidence in the organization - and it is not necessarily due to an Internet-borne incident.

In 2008 many organizations in the Mediterranean Sea basin and in the Middle East suffered Internet downtime due to damages to the underwater Internet cables. Some of these organizations relied on a single Internet connection, and their business was driven by Internet communications. Having such a single point of failure proved to be very damaging for these organizations in terms of lost productivity and lost business. Reliability is a major concern for most businesses and their inability to address even one single point of failure can be costly.

If an organization is not prepared for a security incident, it will probably not handle the situation appropriately. One question that needs to be asked is: if a virus outbreak does occur, who should handle the various steps that need to be taken to get the systems back in shape? If an organization is simply relying on the systems administrator to handle such incidents, then that organization is not acknowledging that such a situation is not simply technical in nature. It is important to be able to identify the entry point, to approach the persons concerned and to have policies in place to prevent future occurrences - apart from simply removing the virus from the network! If all these tasks are left to a systems administrator, who might have to do everything ad hoc, then that is a formula for lengthy downtime.

Addressing security threats

An anti-virus is not an option

The volume of malware that can hit organizations today is enormous and the attack vectors are multiple. Viruses may spread through email, websites, USB sticks, and instant messenger programs to name but a few. If an organization does not have an anti-virus installed, the safety of the desktop computers will be at the mercy of the end user – and relying on the end user is not advisable or worth the risk.

Protecting desktop workstations is only one recommended practice. Once virus code is present on a desktop computer, it becomes a race between the virus and the anti-virus. Most malware has functionality to disable

your anti-virus software, firewalls and so on. Therefore you do not want the virus to get to your desktop computer in the first place!

The solution is to deploy content filtering at the gateway. Anti-virus can be part of the content filtering strategy which can be installed at the email and web gateway. Email accounts are frequently spammed with malicious email attachments. These files often appear to come from legitimate contacts thus fooling the end user into running the malware code. Leaving the decision to the user whether or not to trust an attachment received by email is never a good idea. By blocking malware at the email gateway, you are greatly reducing the risk that end users may make a mistake and open an infected file. Similarly, scanning all incoming web (HTTP) traffic for malicious code addresses a major infection vector and is a requirement when running a secure network environment.

Security Awareness

A large percentage of successful attacks do not necessarily exploit technical vulnerabilities. Instead they rely on social engineering and people's willingness to trust others. There are two extremes: either employees in an organization totally mistrust each other to such an extent that the sharing of data or information is nil; or, at the other end of the scale, you have total trust between all employees. In organizations neither approach is desirable. There has to be an element of trust throughout an organization but checks and balances are just as important. Employees need to be given the opportunity to work and share data but they must also be aware of the security issues that arise as a result of their actions. This is why a security awareness program is so important.

For example, malware often relies on victims to run an executable file to spread and infect a computer or network. Telling your employees not to open emails from unknown senders is not enough. They need to be told that in so doing they risk losing all their work, their passwords and other confidential details to third parties. They need to understand what behavior is acceptable when dealing with email and web content. Anything suspicious should be reported to someone who can handle security incidents. Having open communication across different departments makes for better information security, since many social engineering attacks abuse the communication breakdowns across departments. Additionally, it is important to keep in mind that a positive working environment where people are happy in their job is less susceptible to insider attacks than an oppressive workplace.

Endpoint security

A lot of information in an organization is not centralized. Even when there is a central system, information is often shared between different users, different devices and copied numerous times. In contrast with perimeter security, endpoint security is the concept that each device in an organization needs to be secured. It is recommended that sensitive information is encrypted on portable devices such as laptops. Additionally, removable storage such as DVD drives, floppy drives and USB ports may be blocked if they are considered to be a major threat vector for malware infections or data leakage.

Securing endpoints on a network may require extensive planning and auditing. For example, policies can be applied that state that only certain computers (e.g. laptops) can connect to specific networks. It may also make sense to restrict usage of wireless (WiFi) access points. .

Policies

Policies are the basis of every information security program. It is useless taking security precautions or trying to manage a secure environment if there are no objectives or clearly defined rules. Policies clarify what is or is not

allowed in an organization as well as define the procedures that apply in different situations. They should be clear and have the full backing of senior management. Finally they need to be communicated to the organization's staff and enforced accordingly.

There are various policies, some of which can be enforced through technology and others which have to be enforced through human resources. For example, password complexity policies can be enforced through Windows domain policies. On the other hand, a policy which ensures that company USB sticks are not taken home may need to be enforced through awareness and labeling. As with most security precautions, it is important that policies that affect security are driven by business objectives rather than gut feelings. If security policies are too strict, they will be bypassed, thus creating a false sense of security and possibly create new attack vectors.

Role separation

Separation of duties, auditing and the principle of least privilege can go a long way in protecting an organization from having single points of failure and privilege creep. By employing separation of duties, the impact of a particular employee turning against the organization is greatly reduced. For example, a system administrator who is not allowed to make alterations to the database server directly, but has to ask the database administrator and document his actions, is a good use of separation of duties. A security analyst who receives a report when a network operator makes changes to the firewall access control lists is a good application of auditing. If a manager has no business need to install software on a regular basis, then his or her account should not be granted such privileges (power user on Windows). These concepts are very important and it all boils down to who is watching the watchers.

Backup and Redundant systems

Although less glamorous than other topics in Information Security, backups remain one of the most reliable solutions. Making use of backups can have a direct business benefit when things go wrong. Disasters do occur and an organization will come across situations when hardware fails or a user (intentionally or otherwise) deletes important data. A well-managed and tested backup system will get the business back up and running in very little time compared to other disaster recovery solutions. It is therefore important that backups are not only automated to avoid human error but also periodically tested. It is useless having a backup system if restoration does not function as advertised.

Redundant systems allow a business to continue working even if a disaster occurs. Backup servers and alternative network connections can help to reduce downtime or at least provide a business with limited resources until all systems and data are restored.

Keeping your systems patched

New advisories addressing security vulnerabilities in software are published on a daily basis. It is not an easy task to stay up-to-date with all the vulnerabilities that apply for software installed on the network, therefore many organizations make use of a patch management system to handle the task. It is important to note that patches and security updates are not only issued for Microsoft products but also for third party software. For example, although the web browser is running the latest updates, a desktop can still be compromised when visiting a website simply because it is running a vulnerable version of Adobe Flash. Additionally it may be important to assess the impact of vulnerability before applying a patch, rather than applying patches religiously. It is also important to test security updates before applying them to a live system. The reason is that, from time to time, vendors issue patches that may conflict with other systems or that were not tested for your particular configuration. Additionally, security updates may sometimes result in temporary downtime, for

example when they require a machine reboot. Systems administrators often have to choose between installing security updates immediately and keeping the system up and running.

Minimize exposure

Simple systems are easier to manage and therefore any security issues that apply to such systems can be addressed with relative ease. However, complex systems and networks make it harder for a security analyst to assess their security status. For example, if an organization does not need to expose a large number of services on the Internet, the firewall configuration would be quite straightforward. However, the greater the company's need to be visible – an online retailer, for example – the more complex the firewall configuration will be, leaving room for possible security holes that could be exploited by attackers to access internal network services.

When servers and desktop computers have fewer software packages installed, they are easier to keep up-to-date and manage. This concept can work hand in hand with the principle of least privilege. By making use of fewer components, fewer software and fewer privileges, you reduce the attack surface while allowing for security to be more focused to tackle real issues.

Conclusion

Security in small and medium-sized businesses is more than just preventing viruses and blocking spam. In 2009, cybercrime is expected to increase as criminals attempt to exploit weaknesses in systems and in people. This document aims to give managers, analysts, administrators and operators in small and medium-sized businesses a snapshot of the IT security threats facing their organization. Every organization is different but in many instances the threats are common to all. Security is a cost of doing business but those that prepare themselves well against possible threats will benefit the most in the long term.