TEN WAYS

the IT Department Enables Cybercrime

CDW

KASPERSKY lab

Ten Ways the IT Department Enables Cybercrime

We hope that by now you've already read Kaspersky Lab's whitepaper, "Waging War at the Endpoint." If not, please download and read that whitepaper prior to proceeding (in the resource section.) "Waging War At The Endpoint" focuses on the real target for cybercriminals today—the endpoint, or the employee. This whitepaper focuses on how IT unknowingly enables cybercrime by giving cybercriminals access to systems and data through a series of misconceptions and false assumptions.

End-user demands for access to the World Wide Web and all of the communication vehicles that it affords are at an all-time high. Business demands for those same communication vehicles are also on the rise. The mobility of employees and company data present a growing challenge and keeping up with the exponentially growing cybercrime threat is daunting.

As a result, and often without their knowledge or understanding, many IT departments have become accomplices to cybercrime. This document explains the various ways that corporate IT departments are enabling cybercrime in our environments, and provides some guidelines to prevent this dangerous, destructive practice from continuing.

This paper discusses 10 ways that IT departments are enabling cybercriminals today, and offers ways to stop them, based on third-party research and analysis from Kaspersky Lab experts. How does your organization measure up to these all-too-common pitfalls?

Enabler #1

Assuming the data is in the data center

Consider the fact that most corporate executives have one copy of their email on their smart phone (iPhone, BlackBerry, etc.), a second copy on their laptop, and a third copy on their corporate mail server. This clearly demonstrates that there is twice as much data outside the data center as inside the data center. Add to that the numerous USB memory sticks, CDs, backup tapes, cloud-based solutions, and data exchange interactions with business partners, and this number easily grows beyond what we normally consider.

We innately realize that data isn't contained, yet corporate IT departments treat it as though it were. Why else would we spend disproportionate time and money reinforcing the datacenter perimeter with technologies such as authentication, access management, firewalls, network intrusion prevention, etc.? That is not to say that any of these technologies aren't important. They definitely are. But, we need to concentrate on where our data currently resides; out on the endpoint.

Data does not live in silos. It moves freely outside the datacenter. In fact, IDC research shows that desktops/laptops represent the most serious concern for Data Loss Prevention (DLP). The endpoint represents a more immediate threat to data loss. IDC data also shows mobility is the number one-factor driving new security spending, suggesting that more organizations are taking heed and beefing up security measures beyond their datacenter perimeters.

Enabler #2

Failure to recognize the value of data on mobile devices

Your time is valuable. The countless hours we spend creating reports and analyzing data to make solid business decisions, the weekends we spend on email and on presentations, and performing due diligence on business opportunities that are time sensitive; all of these result in massive amounts of data loaded on portable systems.

Yet, IT departments treat a laptop as a glass bottle of Coke. When a device is lost or stolen, the insurance claim only considers the value of the empty bottle, ignoring all the valuable data that was contained within the device.

Because of that, the protection schemes on mobile devices usually address the value of the device, instead of considering the value of the data. The fact is that most often the value of the data on the device exceeds the value of the devices itself, often hundreds of times over.
Use of managed anti-malware, anti-theft and privacy technologies for mobile device is a good start to address protecting mobile data.

There is a trend among businesses to allow users—beginning at the executive level—to select the make and model of their choice when buying a business-critical mobile device such as a laptop or smart phone. The growing number of iPhones supported on corporate networks is a prime example.

Unfortunately, most business people and IT shops are more concerned with the cost and time for replacement of the device rather than the value of the data on the device.
Employees are equipped with the device of their choice instead of a device that is optimized for managed anti-malware, anti-theft and privacy technologies. The result is an expanding variety of devices, operating systems, carriers, security profiles, and other technologies within the business network. For organizations with a limited security staff, the demand to guarantee cross-platform security can exceed their capacity for support.

Enabler #3

Treating laptops and mobile devices as company assets that are never used for personal use, believing that company data never finds its way to home systems

A few years ago, our corporate IT networks were defined with a solid perimeter. Protection technologies clearly delineated what was internal to the network, and what was external, much like a moat around a medieval castle. External devices were considered untrusted, and those inside benefitted from the protection of the corporate firewall, much like the castle walls.

Businesses worldwide are seeing increasing benefits from empowering remote or mobile workers. Advances in mobile technology have allowed companies to create an "ever-connected" worker who can have full access to critical corporate resources, such as applications, documents, and email, from anywhere in the world, as they travel. That access includes handheld devices.

Mobile employees access corporate networks and data from airport lounges, hotel rooms and in-flight Internet connections—all of which are insecure. Consequently, the common workday is hardly restricted to 9 to 5 anymore. People are working—accessing the most up-to-date information, responding immediately to client contacts, and taking care of many more daily tasks—around the clock. However, this environment has created a new corporate vulnerability that is likely to be targeted by emerging threats (Mobile Security – IDC.)

A strong security policy for a laptop computer fundamentally differs from one for a desktop computer. Often, desktop computers that are used only within the business place don't need certain technologies, such as individual firewalls. But laptops need situational awareness.

When they leave the relative safety of the business network, security enhancements should be automatically programmed to "switch on." Security measures—such as enabling a firewall, disabling non-password-enabled Bluetooth and wireless connections, and increased scrutiny of USB devices—should be automatically engaged whenever a laptop is taken out of the company network.

Enabler #5

Adoption of Social Media without protection

Social Networks are here to stay. This is the new "must have" technology that segments of your business are demanding for growth. When properly used, it can help tremendously.
Ten years ago, the pressure on IT departments was for basic Internet access. Then the demand came for corporate email, and then for Instant Messaging applications. Each of these eventually became mission-critical business tools. Social media is merely the next wave, and we need to be prepared for it.

Many organizations are struggling with the question of how to allow their employees to use Web 2.0 tools responsibly without sacrificing security and regulatory compliance requirements. Social media and Web 2.0 technologies, if used securely, can help organizations increase collaboration and productivity and drive revenue. The focus should be on how organizations should embrace social media in a secure fashion because, with a few exceptions, the outright banning of social media will eventually prove impractical.

A formal policy to control the access and management of social media is essential. For example, if a company protects its perimeter against malware attacks but lacks adequate control for social network access, one employee's carelessness could lead to malware infecting the company network and causing significant economic losses, either directly or indirectly. Social networks are also a possible means for information leaks by employees who voluntarily share information with third parties.

With the exception of some very controlled academic environments, banning social media will eventually prove impractical. A more practical approach is to employ technology that closely watches the traffic that traverses social media websites and blocks known malicious sites.

Enabler #6

Focus on Protection vs. Detection and Response

Consideration of comprehensive security schemes involves multiple capabilities. These basic capabilities are protection, detection and response. Anti-virus products are often overlooked, considered to be commodities, and automatically renewed annually. This results in the quality of detection and response capabilities also being overlooked. As we have demonstrated, these are imperative elements in your security strategy. And, there is a vast spectrum of Protection, Performance, Manageability, Deployment Capability and Support in the industry.

The focus of many organizations is shifting to newer security technologies, such as DLP, Encryption, etc. While those are helpful tools, the overall number of malware incidents and infections continues to grow. An IDC survey found that 46 percent of organizations experienced an increase in malware incidents, while only 16 percent experienced a decrease. The SMB environment (500–2,499 employees) had the most dramatic difference, with 44 percent seeing an increase in malware and only 7 percent seeing a decrease.

That means malware is still slipping through these enhanced prevention measures, demonstrating that increased emphasis must be paid to detection and response capabilities. IT departments have invested in protection mechanisms at the gateway, yet open up wide doors for employees to surf the Web without the proper detection mechanisms in place to ensure that criminals are detected and effectively blocked.

Because cybercriminals today target the endpoint, robust detection and response technology needs to be deployed at the endpoint to protect it from malware designed by cybercriminals to steal data, credentials and revenues.

Enabler #7

Failure to foster a culture of awareness

End-user awareness and training are critical at all stages and levels of information security. For example, employees must be taught how to defend themselves against malicious code—safe surfing, avoiding spyware and scareware, attachment etiquette. Password policies must be evangelized and enforced. Web usage policies must be clearly communicated, monitored and enforced.

Awareness of threats, their impact, and proliferation methods helps keep users vigilant and deters them from making poor decisions that could infect their endpoint. Security awareness campaigns on a recurring basis are vital to keeping employees informed and protected. Of course it is of great importance that the IT staff is well educated on current threat technologies and vectors so that they can make knowledgeable decisions on protection and prevention technologies.

Enabler #8

Under-reporting of security breaches

Although cybercrime security breaches increased more than 23%, and the cost of those breaches has more than doubled, this is only the tip of the iceberg. This data, released by the FBI, is misleading because companies generally do not report when they have been breached. Companies simply do not want the world to know they've been breached for fear that their stock, value, brand and reputation would be negatively impacted.

While this impulse to suppress is natural, the result is a skewed view of the growth in threat across the Internet. Under-reporting gives companies the false impression that the malware threat is minimal and that the growth in cybercrime is over-inflated. The reality is that the threat grew well over 23% —the FBI just cannot quantify it because of the unreported breaches that occur every day.

Companies like yours will benefit greatly by knowing of breaches that occur, how they were perpetrated, and how they can protect themselves from a similar attack.

Enabler #9

Settling for compliance

Regulatory compliance and IT security are not always synonymous. You can easily be compliant with a regulatory body yet be very non-secure. Many organizations view malware protection as a check-off item—"I have to have it and I have to maintain it, but that's all I have to do." Regulatory compliance often involves a "top down" approach. A cookie-cutter template typically defines the initiative. The company must look at its products and processes to figure out how they can mesh with the template.

Security, on the other hand, is a bottom-up initiative when done correctly. Whether you are designing a software product or the architecture for your organization's new network, security elements should be included. When you are designing product architecture, for example, just as a good initial pass would describe communication, localization, versions, and so forth, so should it describe the security elements that need to be built into the application from day one. The security elements should be revisited and refined throughout development.

Compliance may provide an illusion of security to those who do not understand the complexities of securing the digital business world. Compliance alone should not be the end goal.

Enabler #10

Assuming everything is OK

Although systems might be bulletproof, ultimately, human beings operate them. In many cases, problems arise as a result of this human element—of simple honest mistakes or a lack of necessary knowledge and best practices. Company personnel should be trained on information management, including how to act in specific situations, how to follow clear, company-wide safety policies and procedures, how to avoid malware by being diligent and careful and, if malware has already broken into the network, how to act correctly to secure data and prevent further losses.

Take a hard look at the probability of a security event in your business. Everything is not okay. We can all do a better job at ensuring our business-critical data does not find its way into malicious hands.

Summary

Every day cybercriminals find new ways to infiltrate the corporate endpoints for the sole purpose of stealing data and money. According to a SANS.org report entitled "The Top Cyber Security Risks" Companies are losing thousands of dollars each day while thinking they are secure.

We can all do a better job at ensuring our business –
critical data does not find its way into malicious hands

500 Unicorn Park
Woburn, MA 01801
866.563.3099
smbsales@kaspersky.com

www.kaspersky.com
www.threatpost.com

KASPERSKY lab