Office Space: Is there a Peter Gibbons in your office?

The correct answer to the question posed is – who cares? In the 1999 movie Office Space, the protagonist, Peter Gibbons, works for Initech, a firm that updates financial systems to be Y2K-compliant. Bored and completely disengaged at work, Gibbons enlists a couple of his soon-to-be laid off colleagues—Michael Bolton (not the singer) and Samir Nagheenanajar (it isn't hard to pronounce)—to implement an exploit on a credit union and slowly accumulate a few hundred thousand dollars without raising any flags.

The scheme relies on the fact that banking transactions frequently extend out to fractions of a penny. The trio plans to install a virus on the mainframe that will modify the credit union's software to round off those fractions of a penny and deposit these small amounts into a bank account. The difference on each transaction will be less than a penny, but the aggregate from thousands of transactions each day will eventually accumulate to hundreds of thousands of dollars.

Since resources are stretched thin as IT personnel focus on the looming Y2K crisis, no one will ever notice these seemingly imperceptible micro-transactions. This type of exploit, referred to as "penny shaving" or "salami slicing," has appeared in several movies (the characters in Office Space talk about it being used in Superman III) and has even been used in real life.

The modern office space

But much has changed in the past 20 years, including the ability for computers to count above 99 when calculating dates. Architectures are drastically different, with cloud resources, virtual machines, and remote desktop solutions. Security strategies are more comprehensive and involve greater levels of monitoring and threat protection. Workflows are better-defined and user privileges are managed with greater control. The upshot? Peter and his partners in crime would have a tough time pulling off their scam today.

To understand why, let's look at the attack vectors. Michael Bolton writes a virus and explains "all we have to do is load it anywhere into the credit union mainframe and it'll do the rest." He copies the virus to a floppy disk and Peter then copies the virus from the disk to the mainframe.

With today's compliance regulations pertaining to the financial industry and personal information, employees of a modern-day Initech would be using secure thin clients to log into virtualized desktop environments. These thin clients would in all likelihood block external storage devices like USB drives.

(What's a floppy disk?) Even if Peter were able to connect a USB device, there would likely be a moat between the client system and the virtual desktop. In other words, even if he could get the virus onto the client, he wouldn't be able to copy it from the client to the virtual desktop that's accessing the mainframe. This layer of security is a major advantage of using thin clients and a virtual desktop infrastructure (VDI).

There's also a good chance the antivirus protection being run on the Initech systems would block any unsigned executable files on a portable storage device.

Security in a virtualized world

But just for fun, let's assume that the thin client protocols are super relaxed. That still leaves all the security and monitoring protocols in place at a data center. When applications and workloads are centralized in the data center, IT can provide a greater level of monitoring. Individual user activity is monitored, so threat protection in the data center would likely stop a user from introducing an unknown executable into the network and would log any activities, giving complete transparency into any attempt to commit this sort of fraud.

Even more likely, the network would be architected to minimize the threat of an internal attack. Applications, data storage, and other services would be separated into different virtual machines (VM) and zones. Loading the virus "anywhere on the mainframe" wouldn't work in this architecture. Meanwhile, IT would manage very granular permissions for users to prevent a person from accessing any information not relevant to their role. A person working in a database, for example, wouldn't have access to application code.

And following common best practices, Initech employees wouldn't have access to production servers. Instead, they would be checking changes into a sandboxed environment located in an isolated virtual machine. Peter Gibbons would not be able to copy the virus directly onto a credit union server handling actual transactions.

Adding up the numbers

Today's environments perform sophisticated, automated checks. A financial system like the one Initech was working on would monitor transactions and constantly check data integrity. If just one transaction (let alone thousands per day) did not match exactly to the fraction of a penny, the system would send an alert. Other solutions will compare VM to VM snapshots to detect changes.

If any of these problems are detected, recovery is streamlined with virtual machines. VMs can easily be restarted, systems can be rolled back to snapshots of complete unaffected virtual machines, and patches (if necessary) can be quickly applied to virtual systems and deployed throughout an entire environment.

Of course, a big part of Office Space is the work environment – a cluttered, cubicle-filled room where every cramped work space is a jumble of stacked paper, boxes and binders, bulky monitors, CPUs, and massive printers. Here, too, technology has rescued us from the chaos that reigned in most office cubicles of the nineties. The paperless office is a reality, and with today's thin client solutions workspace hardware is minimal, allowing space and resources to be devoted to tools that provide superior ergonomics, most notably larger monitors – where virtually all our work takes place today – such as the

LG 38-inch curved ultrawide thin client monitor that allows you to see far more information than on a smaller monitor and minimizes window management.

Conclusion

Technology is not invulnerable to attacks, but software and best practices are continually growing more sophisticated. With more knowledge, more advanced solutions, and improved workflows, organizations can minimize the likelihood of common security threats.

System monitoring, automated data integrity checks, and comprehensive logging ensure that system health isn't dependent on the availability of human resources to actively look for and detect issues. Virtualization adds additional layers of security and offers enhanced capabilities for blocking and recovering from exploits.

The Office Space scheme all started with a floppy disk, clearly showing that the most vulnerable element in an IT environment is its users—whether intentional or accidental. The entire "penny shaving" exploit could have been prevented if Initech used thin clients. Although, Milton would probably have still burned the building down.

Note: No staplers were harmed in the writing of this article.