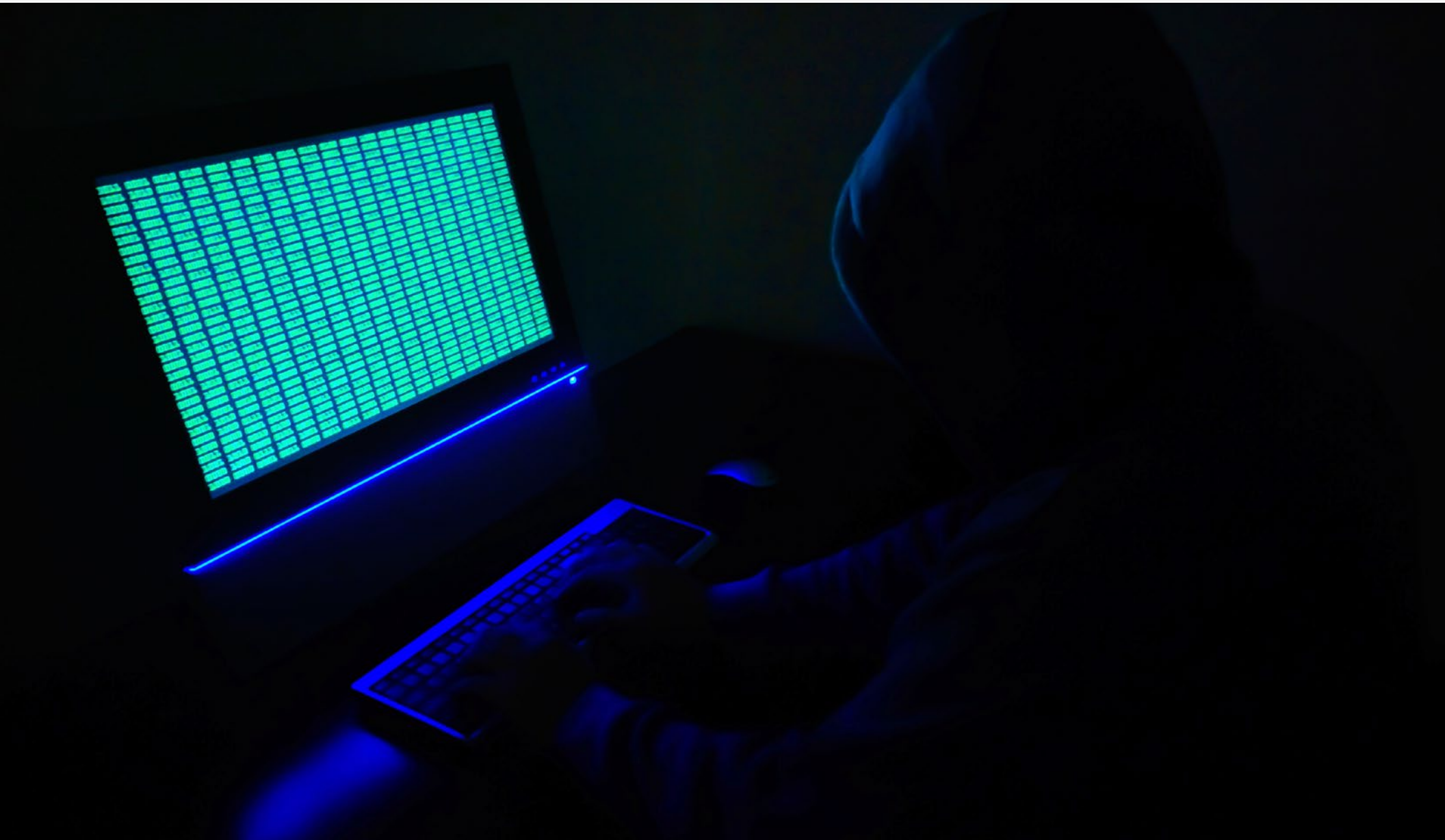
Think HR
Human Powered

CYBERSECURITY
PART 4: VIRUSES AND MALWARE



Think HR
Human Powered

CYBERSECURITY PART 4: VIRUSES AND MALWARE

Corporate networks in companies of all sizes are under siege by a growing number of increasingly sophisticated attacks from cyber criminals across the world. These attacks can happen at any time, both to your business or to you personally on your own private networks. There are steps you can take to reduce the risks as the first line of defense against data breaches, malware infiltration and various other security risks.

This is Part 4 in the series of prevention steps you can take to help make your information networks more secure.

Things have changed over the past few years...cyber criminals are now focusing increasingly on you and your fellow users as the weak link in the security chain.

You...

are the primary line of defense in preventing really bad stuff from happening in your company and to yourself.

There is nearly a one in four chance...
that you will mistakenly click on a phishing email.

One click on a phishing email...
could cost your firm $377 per employee.[1]

A single Trojan horse exploit...
caused the State of California to shut down a business a few days after the attack occurred.[1]

One stolen laptop...
from the car of an HR professional who worked for Godiva Chocolatier revealed the names, addresses, Social Security numbers and drivers' license numbers of other employees.[1]

Edition: 4.2116

What Are We Talking About?

A virus is malicious code that can replicate itself with a variety of consequences, ranging from simple annoyance to theft of data and, in some cases, complete disablement of a computer. Similarly, malware is malicious code that is intended to steal data, record user activity (such as keystrokes), or cause a system to fail. Viruses and malware are typically created by cyber criminals for the purpose of infiltrating your computer, the databases you use, your file stores and other repositories of sensitive or confidential information, but they can also be part of a state-sponsored attack with more strategic objectives. The Stuxnet worm, for example, was a highly sophisticated piece of malware that was designed to infect a particular type of Siemens controller used in the Iranian nuclear weapons program.

Ransomware is a type of malware that can encrypt the data on your hard drive and then demand payment within a limited period of time for the decryption key. Without payment, the files become permanently inaccessible.

While nothing can completely prevent viruses, malware and ransomware from infecting a computer, there are some things you can do to significantly reduce the chance of infection.

The Damage They Can Cause

Viruses, malware and ransomware can cause enormous damage. For example:

- One of the most damaging viruses was ILOVEYOU, written by two programmers in the Philippines. This virus, which was spread using phishing techniques, would overwrite files on victims' computers, rendering them unbootable. The virus infected more than 45 million computers worldwide, and one estimate placed total damage from ILOVEYOU at $10 billion.[2]
- Zeus is a particularly damaging type of malware that performs both keylogging and form grabbing, and was responsible for the theft of login credentials from a wide variety of websites, email systems, social media properties and bank accounts. Tens of millions of dollars have been drained from financial accounts using Zeus and its variants.
- Ransomware, the most common of which is CryptoWall, caused $18 million in losses for the 15 months ended June 2015 according to the FBI Internet Crime Complaint Center;[3] the Cyber Threat Alliance estimates that CryptoWall 3.0 has cost victims up to $325 million.[4] Victims typically pay anywhere from a few hundred dollars to as much as $10,000 to regain access to their encrypted files. Ransomware can be spread through various means, including phishing emails, but can also be spread through bogus software updates.

Edition: 4.2116

How to Defend Yourself

While nothing can completely prevent viruses, malware and ransomware from infecting a computer, there are some things you can do to significantly reduce the chance of infection:

KEEP YOUR SECURITY SOFTWARE UP TO DATE.

While a software update can potentially be bogus, it is essential to apply updates to operating systems, security software and other software as soon as possible after they are published (this is particularly true for plug-ins like Adobe Flash that are highly vulnerable to exploits). Vendors are continually updating and improving the security of these software systems, and so applying updates can prevent some types of infection.

DON'T CLICK ON LINKS OR OPEN ATTACHMENTS

It is essential never to click on links or open attachments from unknown or suspicious sources, since doing so can introduce viruses, malware or ransomware onto a computer and into a corporate network.

NEVER USE USB FLASH DRIVES FROM UNKNOWN SOURCES

USB flash drives help you to share files, take work home, or distribute content to customers and prospects. They are commonly handed out at trade shows and conferences, but are a common source of infection. For example, an analysis of 50 USB flash drives that were found on trains in and around Sydney, New South Wales found that two-thirds of them were infected with some form of malicious software. More recently, the control systems for two power generation facilities in the United States were infected with malware that had been introduced by USB flash drives.[6]

PERFORM REGULAR BACKUPS

Finally, performing regular backups of all computer systems allows recovery from a virus, malware or ransomware infection. By reinstalling the operating system on an infected computer and restoring files from a pre-infection backup, you can go back to a point prior to the infection. While this may result in some data loss, it can restore a computer almost completely to a known good state.

It is essential never to click on links or open attachments from unknown or suspicious sources, since doing so can introduce viruses, malware or ransomware onto a computer and into a corporate network.

Edition: 4.2116

References

1 http://www.privacyrights.org/data-breach
2 http://www.cnet.com/news/experts-estimate-damages-in-the-billions-for-bug/
3 http://www.usatoday.com/story/tech/2015/06/24/fbi-ransomware-cyptowall/29215237/
4 http://searchsecurity.techtarget.com/news/4500256544/Cryptowall-30-reported-to-cost-victims-325-million
5 http://www.paretologic.com/resources/newsletter/usb_drives_spreading_viruses.aspx
6 http://arstechnica.com/security/2013/01/two-us-power-plants-infected-with-malware-spread-via-usb-drive/

Edition: 4.2116

About ThinkHR

ThinkHR provides expert HR knowledge solutions designed to help people and companies thrive. Combining the best of human expertise and innovative technology, ThinkHR's solutions include the industry's first and most used HR hotline, an award-winning online HR knowledge base, and a comprehensive eLearning platform.

ThinkHR's mission is to give its partners a powerful competitive advantage to help them strengthen their client relationships, manage risk and win more business. Equally important, the company is passionate about empowering HR professionals and other executives to become more efficient, productive and successful.

For more information, visit thinkhr.com

ThinkHR
855.271.1050
contact@thinkhr.com

About Osterman Research

Osterman Research provides timely and accurate market research, cost data, cost models, benchmarking information and other services to technology-based companies. We do this by continually gathering information from IT decision-makers and end-users of information technology through in-depth market research surveys. We analyze and report this information to help companies develop and improve the products and services they offer, and to help organizations make better decisions about their security, archiving and other capabilities.

For more information, visit ostermanresearch.com.

© 2016 Osterman Research, Inc. All rights reserved.

This document is offered for general best practice information only. It does not provide, and is not intended to provide, legal advice.

Edition: 4.2116