CommunityIT Innovators® where technology meets mission

IT SECURITY FOR NONPROFITS

COMMUNITY IT INNOVATORS PLAYBOOK

April 2016

Community IT Innovators
1101 14th Street NW, Suite 830
Washington, DC 20005

The challenge for a nonprofit organization is to develop an appropriate security plan that recognizes the difficulty in managing the security of their data assets, engages their staff with sensible practices as an important line of defense, and keeps costs effective.

Whether hiring a Managed Service Provider (MSP) or using an in-house IT Department, organizations need to establish a good foundation of updated systems, regular backups, good user training including passwords, and effective written security policies that can evolve with the organization.

These steps are the Community IT Innovators approach to creating a multi-layered foundation of security.

Table of Contents

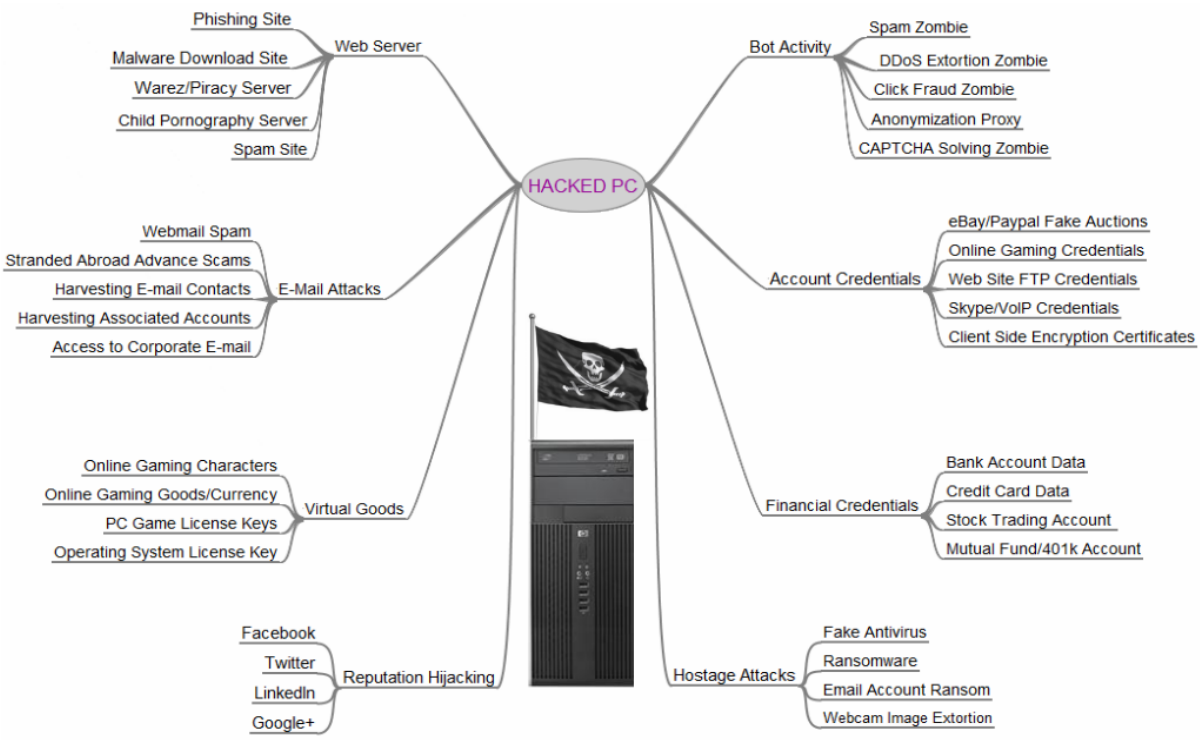
> Nonprofits can't hide in the herd. In fact, many hackers have discovered that nonprofits make good targets. They are easier to penetrate than large companies with security teams and less likely to catch a hacker in the act. Today, most hackers are part of professional rings focused on the bottom line. If there is money to be made by hacking your nonprofit, they won't hesitate.
>
> Idealware Report *"What Nonprofits Need to Know About Security"* December 2015

Introduction

We live in a world with increasing IT Security risks. Recent years have seen a dramatic increase in the change and innovation of the technology tools available to mission driven organizations, but, at the same time, the tools available to cyber criminals have also grown in sophistication. Networks can no longer be protected by a firewall at the edge of a network. The end user's device has become the perimeter.

Begin by dismissing the notion that nonprofits are not targeted or that your organization is safely under the radar because of your size or the unimportance of your data. Attacks have become so automated and hacker code is so available and cheap that every computer and device is a target.

Security threats have evolved into sophisticated and profit driven enterprises with significant resources for cyber criminals. Understanding the new and persistent threats that exist is a good first step to adopting a meaningful approach to security at your organization.



Courtesy of http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Our Approach

People

Most employees will not think IT security is more important than easily and effectively getting the job done.

"What Nonprofits Need to Know About Security" from Idealware covers the basics of user-focused security training, as does the Community IT webinar from September 2015 http://www.communityit.com/resources/webinar-end-user-training/ .

> Passwords are already one of the least secure protections we have available to us. There's every chance you're bad at them to begin with, and the more people who have the key to your alphanumerical digital lock, the more potentially exposed you become – WIRED, February 2016

Passwords should be long and contain a variety of letters, symbols and numbers. All user-chosen passwords must meet the following complexity requirements:

- Must contain at least one alphabetic, one numeric and one symbol character.
- Must be at least 8 characters in length.

Ideally passphrases should be used to increase length. Increased length provides more security than complexity and is easier for a human to memorize. For example, the seven extra characters in Blue5Chandelier2@ make it 64 trillion times stronger than lf@j7asFd!

Privileged accounts (typically domain admins) should be optimized for security since no human needs to memorize these passwords. The account names should also avoid using common Admin names (such as support, exchange, admin, etc) to reduce the surface area of attack for brute force attacks.

Administrator level passwords with privileged access:

- Should maximize the possible length of password for each platform.
- Should not be memorized.
- Should avoid passphrases (ie. quickbrownfoxjumpedover) to discourage memorization.

Using complex passwords is a challenge, so the use of a password manager is required. Solutions such as Secret Server Online, Last Pass or Dashlane are indispensable.

Process

Nonprofits of any size need a set of written IT security policies – but in our work with clients we've learned that many have outdated policies that no one references and staff who don't know what the policies cover, or realize too late they don't have a policy at all.

You should have **Written and Updated Security Policies** tailored to your organization. These policies should be viewed as living documents that are regularly updated to reflect changes in technologies, priorities and assets.

Your staff should be familiar with your IT Security Policy, should understand the reasons for your policies, should know how to consult your Security Policy or IT Providers if they have questions, and should be regarded as your principal asset in keeping your IT safe and secure. You and your IT provider, or IT department, should be conducting regular **Staff Training and Awareness** and sharing

information on new procedures and threats to engage users in creating a collective culture of security responsibility.

Written policies are not only protection against misunderstandings; creating up-to-date policies can be an instrument for proactively assessing risk, assigning access, and enlisting staff as your first line of defense against hackers and disasters.

Community IT Innovators employs the CIA security framework with our clients - this stands for Confidentiality, Integrity, and Accessibility. The CIA framework helps you assess your data and assign risk levels. Community IT presented a webinar in 2015 on Crafting an IT Security Policy for Your Nonprofit http://www.communityit.com/resources/webinar-april-2015/ The webinar takes you through a manageable outline to create or update a policy for your organization addressing different levels of access to data, confidentiality and security, and what policies need to be in place for staff mobile devices.

Technology

An effective security strategy requires a multi-layered approach. At Community IT Innovators we combine people and process elements along with robust technology solutions to build an effective security framework.

Patching

Community IT deploys patches from a cloud platform, where we constantly monitor and manage software, ensuring definitions are kept up-to-date and active. Our best practice is to patch workstations weekly and servers monthly.

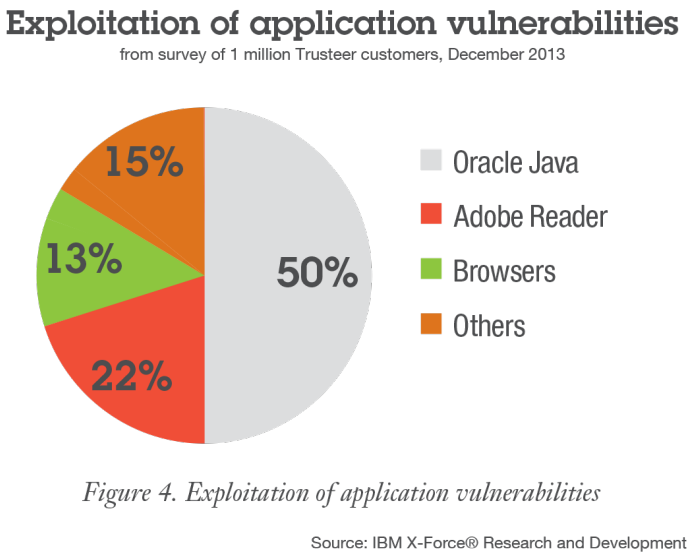


Figure 4. Exploitation of application vulnerabilities

We know that most attacks are perpetrated by exploiting vulnerabilities in the operating system and third party applications such as Java, Flash and Acrobat. A security study by IBM indicated that the vector of application vulnerabilities has shifted over time from being primarily directed at Windows and related Microsoft applications to being directed against a wide range of third party applications.

Our Community IT Innovators team communicates in real time with our client contacts, keeping them informed and updated on our security decisions, because we believe our clients can't participate in security if they view security as *something someone else does*.

Antivirus

Contemporary research shows that Antivirus is stopping only about 40-50% of malicious software. We do expect to see improvements in Antivirus effectiveness over time and still view the software as a key component of an effective security strategy.

Our cloud based management platform fills a dual role of both deploying antivirus and monitoring its effectiveness and status. Through this two-pronged approach we are able to identify those systems that lack protection or are not receiving the most up to date virus definitions.

Backups

If disaster strikes, or you are compromised by a disgruntled employee or hackers demanding ransom, you will need to restore from your most recent backup. A good backup strategy is a key component of an effective security plan. Community IT Innovators sets up a backup regime with both Recovery Point Objectives and Recovery Time Objectives. We backup email, databases, and cloud data as well as on-premise data.

Your organization should never be conducting a restore for the first time after a disaster. Community IT Innovators regularly conducts test restores and shares the results and learning from these trial runs with clients. Find more resources from our recent webinar here: http://www.communityit.com/resources/webinar-february-18-2016-backups-and-disaster-recovery-for-nonprofits/

Predictive Intelligence

Predictive intelligence seeks to proactively defending your systems against new attacks and threats. Predictive Intelligence firms both crunch big data to identify ongoing sources of attacks, and also react nimbly and immediately as new threats emerge. If you don't employ Predictive Intelligence in your arsenal of defense you become limited in your ability to keep hackers out, and can only react when your systems are already compromised.

Community IT deploys a predictive intelligence layer powered by OpenDNS. OpenDNS provides zero latency protection against web-based attacks. All DNS queries are resolved by the service and malicious traffic is blocked and reported.

More resources from http://www.communityit.com/resources/2016-jan-it-security-threats/, a free webinar presented in January 2016.

Summary

Ask your IT Provider, Managed Services Provider (MSP) or IT Department about

People

- Ask them to perform **User Security Training and Awareness** often.
    - Trainings should include the physical security of your IT assets - locked doors, proper passcode security with mobile devices, and what to do when IT assets are compromised.
    - Training should include compliance with written Security Policies.

- Ask them to explain in laymen's language the security steps they take, and be wary of an IT security head who wants blind trust; your provider should view your organization and your staff as vital partners in your security approach.

- Ask your IT Provider how to contact them when you suspect a problem, how long they take to respond, and what response levels are covered by your contract.

Process

- What is our **Written IT Security Policy**? How often will it be updated?
- How do they help comply with any external compliance or regulatory requirements?
- How and when do they perform a data inventory?

Technology

- How they perform emergency **Patches** as issued for known security vulnerabilities
- Which **Antivirus** they use and why
- How they utilize **Predictive Intelligence**
- How they perform **Backups**, how often, and how often they practice restoring from backups
- How they manage **Passwords** for users and Admin accounts
    - Is your password and account access policy robust enough?
    - Do you require 2-step authentication for access to systems?

About Community IT Innovators

Community IT Innovators is a Washington, D.C. based IT consultancy providing technical staff and strategic technology support to nonprofit organizations. Community IT have focused exclusively on nonprofit technology since 1993, and have a staff of about 40 providing the depth and expertise needed for the broad range of technology management challenges unique to nonprofits. Community IT is the only company from among the top 200 managed IT services providers in North America that is focused exclusively on nonprofit technology support, with certifications in all of the major (and some less common) technologies in use at nonprofit organizations today. Community IT serves customers primarily in the DC and Baltimore areas, with customers ranging in size from a few staff to several hundred. For more information please visit http://www.communityit.com

> Hiring a full-time Network Administrator from Community IT is like hiring a whole organization to address our IT needs.
>
> In addition to daily support, we tap into the collective Community IT experience, solutions, new ideas, and best practices.
>
> **Karen Lattea,**
> **Chief Administrative Officer**
> **Sojourners**

Source: Community IT Innovators Help Desk Survey September 2015