IT ONDEMAND
it-on-demand.com

THE TECHNOLOGY TIMES NEWSLETTER

March 2016

This monthly publication provided courtesy of Howard Globus, Security Evangelist & Partner of **IT On Demand.**

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Relying On A Good Luck Charm?

Carrying a four-leaf clover might work for leprechauns. But when it comes to Internet abuse by employees, you're gonna need more than sheer luck…

Did you know that…

- 70% of all web traffic to Internet pornography sites occurs during the work hours of 9 a.m. – 5 p.m.
- Non-work-related Internet surfing results in up to a 40% loss in productivity each year at American businesses.
- According to a survey by International Data Corp (IDC), 30% to 40% of Internet access is spent on non-work-related browsing, and a staggering 60% of all online purchases are made during working hours.

The list goes on, and the costs to your company can be staggering.

What types of web sites present the greatest risk? Categories include abortion, alcohol, dating, death/gore, drugs, gambling, lingerie/swimsuits, mature, nudity, pornography, profanity, proxy, suicide, tobacco and weapons.

Risks these types of web sites expose your business to include malware, viruses, fraud, violence, lawsuits, loss of confidential and/or proprietary data and more. Even social sites, while perhaps not quite as risky, can have a major impact on productivity.

Barriers that once stood at the edges of your office network have been annihilated by digital media.

Web content filtering is now crucial to network security – not to mention employee productivity – in this emerging environment. It can be deployed in a number of ways, but basically they boil down to two: inline and endpoint filtering.

Inline Web Filtering
One way to filter web content is to control it at the entry point or gateway to your network. This technique intercepts all web traffic and applies filters that allow or block web access requests. Because the entire network is filtered, no access to the user's device is required.

Continued on page 2

With inline web filtering, there's no need to expend resources managing content at each endpoint – your employees and their computers, whether desktop or mobile. Inline filtering not only saves bandwidth, it goes a long way toward mitigating cyberthreats. For securing activities that take place within your network, it's a critical and potent strategy.

> *"Any employee can carry an infected machine into and out of your company's building and network on any given day."*

Yet, with the shift away from traditional office-bound work routines to a work-from-anywhere culture, the effectiveness of inline filtering has diminished. When employees access the web outside your network's gateways – via home networks, hotels, coffee shops, etc. – their devices become vulnerable to attack.

And any employees can carry an infected machine into and out of your company's building and network on any given day, exposing your entire intranet to infections. And that's why so many companies are moving to endpoint-based web filtering to complement their inline filtering.

Endpoint-Based Web Filtering

Endpoint-based filtering protects employee devices from infections, no matter where they connect to the web. Software at the endpoint – your employee's device – carries a predefined filtering policy from the central server that can be intranet-based or cloud-based.

The endpoint filter is then updated periodically from your company network. This method assures that web filtering is always active, no matter which gateway the machine connects through. The downside is that it must be rolled out and maintained at all endpoints.

That being said, one advantage of endpoint-based filtering is that it addresses stringent employee privacy regulations that are quickly becoming the norm in Europe and elsewhere around the world. Because it keeps browsing-pattern information within the user's device, endpoint-based filtering provides a fairly non-intrusive way to handle employee privacy concerns.

And finally, while endpoint-based filtering really is the only way to protect a network without boundaries, as most companies now have, ideally it works hand in glove with inline filtering.

Forget the Charms – You Can Bet On This

We highly recommend rolling out not only inline and endpoint filtering, but also an effective training program for your staff to encourage best practices and assure compliance with your company's web security policies and procedures.

Want to make sure all gaps are sealed and you won't have to depend on a four-leaf clover, a rabbit's foot or knocking on wood to keep your network secure?

Contact us before March 31st, 2016 at **(212) 235-0260** or info@it-on-demand.com for a customized Web Content Filtering Review and Analytical Report on your system.

"I've put on a lot of weight, but I'll lose it all in the Spring."

Our Favorite Quotes of the Month

"A man who wants to lead the orchestra must turn his back on the crowd." – Max Lucado

"Twenty years from now, you will be more disappointed by the things that you didn't do than by the ones you did do. So throw off the bowlines. Sail away from the safe harbor. Catch the trade winds in your sails. Explore. Dream. Discover." Mark Twain

"Average leaders raise the bar on themselves; good leaders raise the bar for others; great leaders inspire others to raise their own bar." Orrin Woodward

Virtualization & Disaster Recovery: What Do They Have in Common?

Many business owners think that Virtualization and Disaster Recovery are two separate services. And while that's true in most respects, they actually have more in common than you think. Particularly in how Virtualization can serve as a legitimate Disaster Recovery solution. Here are the details of how it does just that, and some pointers to keep in mind if you choose Virtualization to backup your systems.

As opposed to tape backups, Virtualization reduces recovery time in the event of a disaster. While tape backups can be reliable, using them to fully restore your system after a backup can be an excruciatingly long process. In fact, it can take up to two days to do just that. Think of all the business you could lose in those two days. Think of all the lost money in salaries you'll pay out out to employees who aren't working. Simply put, Virtualization is much quicker than tape backups when it comes to Disaster Recovery. Your entire system can be restored in four hours or less. How does this happen? Well, instead of rebuilding your servers, operating systems and applications separately, they exist safely off-site and can be brought back online via your virtual backup.

While the speed of virtualized backups might sound alluring, there are a few key points you should be aware of before moving forward. Here's what you need to think about:

- **Critical data** - where do you want your critical data to be stored? Do you want it stored on tapes? Disk technologies? Or on your virtualized servers? Perhaps it's best to spread your risk by backing up your critical data to multiple sources because, frankly, your business depends on this data. Regardless, find out what critical data you need to operate your organization and devise a plan to back it up as you see fit.
- **Data to be backed up** - Whether or not you decide to store your critical data on your virtual machines, figure out what data and assets you do want stored on them. Then designate specific virtualized servers to store these assets. In case a disaster does happen, you'll know immediately where your backups live, and can retrieve your data quickly and get your business up and running again fast.
- **Systems to be virtualized** - Just as your business has critical data, you also have critical applications. Some of these may include email, Microsoft Office, and applications or software developed in house. Whether or not these applications qualify as critical for your business, identify the ones that do and focus your disaster recovery efforts on them. Like your data and servers, applications can all be virtualized and then safely stored off-site.

If you choose Virtualization as part of your Disaster Recovery solution, make sure your backups are monitored regularly so they're up-to-date in the event of a disaster. And besides Disaster Recovery, there are many other benefits to Virtualization. Your business can reduce the amount of servers and other hardware in your office, lower your electricity costs, and save money in the process. Consider Disaster Recovery as a nice bonus that's included with these benefits.

Curious to learn how else Virtualization can benefit your business? Interested in a dedicated Disaster Recovery solution? Call us today and discover how our experts can protect your organization and save you money.

Published with permission from TechAdvisory.org

Creating a High Reliability Organization for Your Business

Experts agree: technology alone will not protect your company from cyber threats. In the majority of breaches, human error plays a factor, regardless of how sophisticated the technology may be. However, when paired with up-to-date tools, a company that respects and follows safe cyber practices can drastically improve its security.

The difficulty lies in creating that culture of cybersecurity. In recent years the US military –which faces tens of millions of cyber threats every day – has addressed this very problem by adopting a High Reliability Organization (HRO) methodology. The concept of an HRO came from industries in which even a small mistake could have disastrous results, such as air traffic control and nuclear power plants.

Today, businesses of any type can learn valuable security lessons from HRO practices. These principles include being aware of your vulnerabilities, consistently maintaining high operational standards, being vigilant, and having clear methods of accountability.

HRO's abide by six core values:

1. **Integrity**
2. **Depth of Knowledge (i.e. giving your employees an understanding of the bigger picture of how and why these systems work)**
3. **Procedural Compliance (and inspecting that compliance periodically)**
4. **Forceful Backup (e.g. two-step authentication policies)**
5. **A Questioning Attitude (i.e. encouraging employees of all levels to speak up when something seems wrong)**
6. **Formality in Communication**

If and when incidents occur, it is almost definitely due to one of these principles being ignored. However, each can and should be adjusted to best fit a company's needs.

These principles create a solid foundation from which to build a better-protected business. Be firm and consistent with your security policies, and use inevitable mistakes as an opportunity for everyone to learn. Ultimately, as a CEO engages with and values cybersecurity, a company culture of High Reliability will begin to form.

If you would like guidance or assistance with your security policies, please don't hesitate to contact IT On Demand at (212) 235-0260 or at info@it-on-demand.com. We would like the opportunity to speak with you!