TMC's ADVISOR

Covering IT and Telecom from a Canadian Viewpoint **July 2016 , Volume 3 Issue 7**

Courtesy of freedooom at FreeDigitalPhotos.net

Data Breach Protection

By Peter Aggus

As Hurricane Katrina showed the City of New Orleans, when your single line of defence fails, your entire system is swamped. Segmentation is one way to ensure that a single breach will only compromise a part of your network—but is that enough? How segmented do you have to be? Is implementing multiple VLANs good enough or do you need structured firewalls and routers? Worse than having a breach, is telling everyone that you are well protected … and then still having a breach. How will your network design stand up to an attack?

Read More

Inside

The ROI on IT Assessments

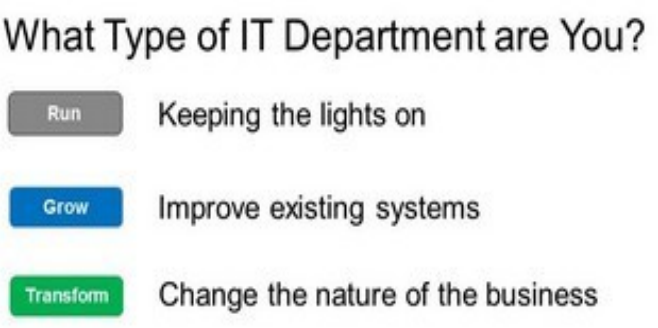
Our clients have hired us to conduct an assessment of their IT operations for a variety of reasons including:

- Investigating reliability problems
- Assessing customer service levels
- Benchmarking costs
- Assessing staffing levels and skills
- Assessing IT Process Maturity

More Information

Contact Ellen for a complimentary copy of **IT Assessments 123**.

ellen@tmcconsulting.ca or 604-506-2905



 ISSN 2369-663X

Data Breach Protection

By Peter Aggus

As Hurricane Katrina showed the City of New Orleans, when your single line of defence fails, your entire system is swamped. Segmentation is one way to ensure that a single breach will only compromise a part of your network—but is that enough? How segmented do you have to be? Is implementing multiple VLANs good enough or do you need structured firewalls and routers? Worse than having a breach, is telling everyone that you are well protected … and then still having a breach. How will your network design stand up to an attack?

Attack Vectors

Attack vectors are the mechanisms available to gain unauthorized access to a network and this includes all of the ways than an intruder can acquire an IP address within the 'subnet' (IP address range) assigned to a network segment. User IP addresses are assigned by a DHCP server and the easiest option is to simply ask for an IP address from the DHCP server.

If the DHCP server has been configured to only issue IP addresses to devices with known MAC addresses, then the intruder will just guess an IP address. Local devices are not intelligent enough to look for intruders, so they will likely have open access to resources on the segment. If the segment includes servers, access will ***usually*** require a login but a determined intruder can often get the information by spoofing a genuine user (pretending to be them).

Segmentation vs VLANs

A LAN segment is the group of devices that can directly 'see' each other. IP packets route between devices in a segment without outside assistance, while IP packets to other destinations need to be routed. Simple networks

Courtesy of freedooom at FreeDigitalPhotos.net

are just a single segment—often bounded by a router provided by their ISP. Unfortunately, many multi-site commercial LANs are set up the same way, using bridges to link buildings in a single partition.

VLANs multiplex several separate user communities (voice, CCTV, etc.) onto a single physical cable. They may appear to behave like discrete segments but as they share common cabling, an intruder with physical access has implicit access to all VLANs on it.

Secure Partitioning

To be secure, segments must only be connected using secured devices (routers or advanced bridges) such that intruders can be identified and blocked. As older network protocols like NetBIOS do not work across subnets, make sure your network protocol is up to the job.

Partitioning with a secured boundary limits intruders to one physical segment. The optimum partitioning will separate business activities so that a compromise to one partition will only affect one business activity.

For example, marketing staff may be configured as one segment, with manufacturing separated into another. Of course, too much partitioning will hamper business—too little is poor security.

Beyond segmenting, your design needs to make sure that all security detecting, blocking and alerting options are activated and, of course, never use out-of-the-box defaults. Intruders like defaults—it is like providing locks and leaving keys under the mat.

This article is reproduced from the July 2016 edition of ***TMC's Advisor***

Peter, as a certified project manager & technology management consultant, has developed innovative & cost-effective solutions for clients in many industries.

Top Shortcomings in Disaster Plans

By Guy Robertson

No matter how careful and intelligent the planner, the best-laid plans often lead to unintended consequences. This is usually because they're often built on theory, rather than experience. For example, in many organizations, the disaster plan is actually called an *Earthquake Preparedness Plan*. Right away you know that it doesn't cover everything that can happen. Our experience, when auditing Disaster Plans, has been that plans are inadequate for even a moderate earthquake.

What's In

If your disaster plan is really an earthquake preparedness plan, then it will include lists of emergency supplies for your offices, and a staff directory with home and cellular telephone numbers. There is the usual advice to duck and cover until the shaking stops and warnings about aftershocks, downed power lines, unstable masonry and broken glass, power outages, and data loss. All of this information is useful, and you should keep it on hand.

What's Not In

Even on the topic of earthquakes, your *EPP* is not likely based on a realistic assessment of the risks to your staff, facilities, and operations. It does not discuss how an earthquake could damage your building—its exterior and interior—or your IT hardware. While it contains information that could be helpful before an earthquake, it does not recommend post-disaster measures that would support your efforts to restore your damaged assets.

But relax! Earthquakes are infrequent. With any luck, you will be able to retire without ever having to re-open the three-ring binder that contains your *EPP*. Unless, of course, there is an earthquake, in which case you and your staff could be in life-threatening trouble.

Biggest Gaps

Your *EPP*'s most glaring gap is that it neglects all risks except earthquakes, including those risks that are more likely to become real physical threats. Earthquakes are more dramatic than flooding from a burst pipe, but such flooding is much more likely to occur. Your disaster planning should cover all of the risks that prevail in your region and community, and at your site including: fire, flooding, gas leaks, toxic spills, high winds, winter storms, power outages, pandemics, data loss, and (of course) earthquakes along with post-disaster shortages of food, water, drugs, and fuel.

Second, your plan is likely impractical as it lacks staff orientation and training tools. You and your staff need to know what to do after any sort of disaster, but your *EPP* contains no educational materials. If an earthquake strikes, your staff might look to you for direction, but you will have had no more training than they have had, and you could find yourself confused and ineffectual.

This article is reproduced from the July 2016 edition of ***TMC's Advisor***

Guy Robertson is a Senior Management Consultant at TMC who specializes in emergency management and disaster planning. He has written extensively on emergency planning and IT security—hundreds of articles as well as two books with worldwide sales.

IT Study Roundup

By Shelley Thompson

A lot of very interesting studies come across our desks each month. We've decided to pull some of our favourites and share the highlights with you. This month we look at a 22% increase in cyber crime, employees who sell passwords, data breaches through employee's mobile access and the economic cost of internet outages.

Cyber Crime Up 22%

According to *Get Safe Online* and *Action Fraud*, the UK's national fraud and cyber crime reporting center, UK businesses have reported a staggering **22% increase in cyber crime** in the past year with losses totalling more than £1 billion.

'Mandate fraud', where criminals persuade employees to change a direct debit or standing order by pretending to be a supplier, is growing particularly quickly, seeing a 66% increase over the past year.

The other type of fraud seeing the largest growth this year is the 'whaling attack', where employees are convinced to make large cash payments to a criminal based on an email that seems to come from a senior manager of the organization. Read More

Passwords for Sale

A *SailPoint Technologies* survey identifies that, surprisingly, 62% of employees would share their passwords with co-workers, and **42% would sell their password** for as little as $150 to a third party.

Interestingly, this information is contradictory as employees are more and more concerned about the security of their own information at the same time as they may be causing security breaches at work.

Read More

Employee Mobile Data Breach

Of Global 2000 companies, the majority do not handle mobile data security properly. Not only do they not have adequate practices in place, they don't even have adequate policies. A recent study by the *Ponemon Institute* found that of surveyed IT and security professionals in the US , 67% stated that it was 'likely' that a data breach had occurred from employees' mobile access in their organization.

Read More

Internet Outages

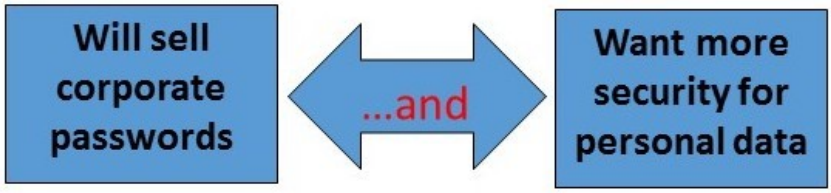
In a study conducted by *Opinium*, 72% of 5.4 million businesses in the UK experienced internet connection failures in the past year. The outages totalled 149 million hours of downtime and **cost the economy £12.3 billion.**

Only 13% of those surveyed were able to use a redundant connection and continue work normally.

Medium to large businesses accounted for the largest share of this total revenue loss as they are the largest users of cloud services.

Read More

The people side of security is tricky as employees:



This article is reproduced from the July 2016 edition of ***TMC's Advisor***

Shelley Thompson is a researcher and business analyst who oversees client benchmarking studies.

Common IP Telephony Scams

By Ellen Koskinen-Dodgson

Telephony Fraud has always been with us as criminals gain access to your telephone system. With the advent of IP telephony, there are many new risks and new requirements for protection.

What They're Doing

Criminals want to take control of your IP Telephony systems for many reasons, including:

- To obscure their 'tracks', by routing calls through intermediate systems before connecting to their ultimate destination
- Access to free international calls
- Resale of international calling
- Rental of a cost-to-call number (similar to a '900' number) in a foreign country, then generating floods of calls from your telephone system to that number
- To launch a denial of service attack on your business

How They're Doing It

All of the traditional ways of accessing your telephone system still apply but now there are new ways:

- Use open source tools to identify systems with weak passwords
- Use standard hacking to access IP telephony systems

Courtesy of Stuart Miles at FreeDigitalPhotos.net

- Make use of known vulnerabilities in specific vendor telephony systems and components such as session border controllers

How to Stop This

There are a variety of ways to protect all of your IP telephony systems and components. These include:

1. Use strong passwords at each risk point including UC clients
2. Use a VLAN for IP telephony traffic.
3. Use blacklisting to block calls to top destinations for fraud such as Cuba, Bosnia, Herzegovina, Latvia, and Somalia, and use whitelisting to permit calling to specific telephone numbers within those countries.
4. For those that have this feature, 'call limiting' can be used to specify that 100 calls per day are allowed to France, but only one to Cuba.
5. You may wish to route unauthorized calls to your security desk for investigation.
6. Of course, keep up to date with the security warnings and stay current on patching.
7. Use your call detail recording to alert you to suspicious calling destinations.
8. Establish alerts when all of your trunks are busy as this can be the beginning of a denial of service attack.

This article is reproduced from the July 2016 edition of ***TMC's Advisor***

Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.