encription
IT Security and Forensic Services

10 Completely Free Activities Every SME can do to Improve Information Security

By Mike Sheward

For smaller enterprises the costs of developing an information security program can be a turn off. In an environment where every purchase is closely scrutinized to determine how it can help the business grow and improve operations. It’s like being 17 and owning your first car; you save up for years, get help from Grandma and finally make the purchase. You feel like you’re on top of the world. Then someone tells you that you need to buy insurance, and you’re brought straight back down to earth!

Truth is, not every security problem needs to be solved with a great big wad of cash. By investing time, taking a step back to assess what you have in terms of infrastructure, and what you are trying to protect, you can really give your security program a shot in the arm.

Ask Your People How They Are Using IT

People come to work to do a job, not to waste hours messing around with a computer. A computer is a tool that should make doing the job easier. If you aren’t providing the right tools, it’s never been easier for someone to go out and acquire their own tools a little or no cost.

For example, if you don’t have remote access to work email, and someone wants to work on a file at home – why not fire it off to their own private email address so they can pick it up later. Not a malicious act by any means, but an act that ensures that your data has left your control. If that data contains sensitive information, this could be identified as a risk item.

Or even more worrying, to gain access to a work machine after hours, they’ll spin up a copy of LogMeIn, GoToMyPC or similar. A remote access tool, which creates a tunnel into your company outside of your control.

Ask your people what tools they feel they need to do the job. In some smaller companies, people often feel nervous to ask for more, especially when they can just get by using free tools that they are already used to using outside of work. Truth is, software used at home might not cut it commercially, either by lack of controls to protect your data, or you may find yourself running foul of licensing agreements.

Get Rid of Your Old Stuff

Hardware, software, data, operating systems or even the coffee machine. Whatever you can think of, if you don't need it anymore to do business, turn it off and remove it from your environment.

Systems placed into production that are no longer a requirement are often kept running 'just in case' they are needed. The problem is, that older systems are often a great vector for attackers. Often forgotten and misunderstood, an old system becomes too fragile to patch, paving the way for point and click exploitation, and a perfect place to begin exfiltration.

Change Administrative Passwords

Every 30 days or as soon as someone who had access to it leaves, you must change your administrative passwords.

It's so simple, so effective and can be done in only a few seconds – so why don't more people do it?

Well the answer to that is, because people often set things (such as scheduled tasks) up to run as an administrator, and the fear is that changing the password will break the process. In my opinion, this is all the more reason to keep the admin account password changing – it might force a change in thinking.

Port Scan Your Network

This is the first of our items that will leverage an open source security tool. Acquire a free port scanner (lets face it, you'll probably use nmap) and use it to sweep your internal IP address ranges.

This is less invasive than a full-blown vulnerability scan. You will gather information on open and closed TCP ports listening on the various IP addresses, and will be able to get a good picture of the hosts connected to your network.

Port scanning once is a great start, but port scanning over and over again will give real value. Set a daily scan to run, and run at different times of the day.

Several scanning tools have a feature that will allow you to compare one set of scan results to another, highlighting changes between scans. In the nmap world, this tool is 'ndiff'. This is a great way to recognize new additions to the network. If you have virtualized infrastructure, you'll no doubt be aware that VM's can pop up from anywhere – so this is a great way to keep tabs on them.

Review Wireless Security

If you have Wireless in your office, double-check your security settings one more time. Long gone should be open, WEP, and WPA encrypted networks. WPA2 with a strong key that is rotated regularly (every 60-90 days).

Oh and by strong key, let's say a string of 32 random characters including upper, lower, special character and numbers.

Yes, it becomes a pain to update devices that connect to Wi-Fi, but most of them have a copy/paste ability these days. Key distribution to authorised personnel should be a piece of cake via internal means.

Most wireless routers will also allow you to set up an isolated Guest network. Do this, and prevent visitors from accessing your internal network. Depending on your policies, this may also be a good option for employee personal devices.

Patch! Patch! Patch!

Ensure regular patching of operating systems, business applications, browsers and browser plugins is taking place. 99.9% of patches include some sort of fix for a security problem.

How can you ensure that this is happening? Use automated patching technologies, such as WSUS in Windows Server to download the latest patches.

Depending on the nature of a server you may need to be cautious in the automatic application of patches, it's a smart move to backup or snapshot a system prior to applying a patch.

Set aside a few hours every couple of weeks to dedicate to patching. Most systems administrators will happily take this task over having to either rush patches when they realise they need to be compliant with a regulatory standard. Or, even worse dealing with the fall out when a security problem is exploited.

Also, it's worth noting that you're more likely to run into a problem applying patches if you've left a long gap between patching sessions.

On end user machines, you can use organizational policies to enforce updates or notifying users to update when a new critical patch is released.

Identity and Access Review

One of my all time favourite horror stories comes from an organisation I was testing. I asked to be given a 'regular' user account to login to an active directory environment. However, I was surprised to discover that with my simple account I was able to browse the personal files of a C-Level executive.

Why? I asked, is this possible?

No one on the IT team could provide an answer, so we began to dig. It didn't take more than 5 minutes to discover that the domain users group had been added to domain administrators group – thus providing a lot of access to a lot of people.

If this organisation had taken a couple of hours every quarter to review the user accounts in their system (there were only about 60), and the permissions assigned to those accounts. This would have not been an issue. Instead, this configuration had persisted for several months, placing the entire system at significant risk.

So what should you look for in an IA review?

- Look for accounts that belong to people that no longer work with you.
- Be sure you know what all service accounts do, and who has access to them.
- If people have changed job roles, ensure that their permissions match their updated responsibilities and have not acquired them extra permissions via permission creep.

There are plenty of expensive systems that track this type of work for you, but it doesn't need to be complex. A simple spreadsheet recording findings can do the trick.

Record Business Process Flows

This is something of an annual or as needed activity. Recording data flows and how they align to business processes will help you be more secure.

You'll get a better idea of what systems use which data, and where they get that data. You'll also discover who has access to that data, and which servers and/or storage locations are involved.

You'd be surprised at how eye opening this activity can be. As a company grows, and new systems are added, it's not long before we lose track of how those systems interact.

Spend an hour - gather a group of people round the table, and draw everything out on a whiteboard, then take a picture and you'll have a handy reference.

In the event of an incident (security related or otherwise) this'll be incredibly useful.

This can also lay the groundwork for a more security-focused activity – developing a threat map.

Encrypt Any Device That Leaves the Office

If someone without permission has physical possession of a laptop or mobile device, at best it's lost forever, worse case, the data on it is compromised.

Things get stolen or go missing all the time; it's going to happen. Therefore, there can be no excuse for not encrypting the entire contents of a hard drive.

All operating systems now include some sort of encryption features, each have varying degrees of effectiveness when deployed.

However, the one safe bet, and one of the most reliable full disk encryption software tools that I recommend is TrueCrypt.

TrueCrypt is completely free, open source software. It can create encrypted partitions on a disk, or simply do the whole drive. If you chose to do the latter your user will be prompted for a key to unlock the drive every time they start up their machine. This can be off-putting, but after a couple of boots, you soon get used to it.

You can also create a recovery CD with a master key that allows an administrator to unlock a drive if needed. Great to know if you need to access a drive in an emergency, or during a forensic operation.

Firewall Rule Review

In a typical SME, firewall rules are not that complex. Every quarter, spend time to confirm that no unexpected rules are in place.

In most cases, this will be an inbound rule or port-forwarding configuration.

Remember, every rule needs a business justification; otherwise it shouldn't be there.

All changes to firewalls should have an audit trail behind them.

Summary

We've just covered ten activities that require little financial outlay, but will provide a big security impact. Of course, not every suggestion will fit every organisation – we are all different, but they should provide a good starting point for just about any SME.

Some of these activities align perfectly with the requirements laid out in security standards such as PCI-DSS and ISO 27001, so they'll give you a boost if you plan on subscribing to any of these. Of course, you might not always plan on it; it may suddenly become mandatory depending on whom you do business with!

Remember, simple controls are better than no controls at all, or controls that are so complex you don't maintain them.

Build a program that aligns to your business objectives, and your people won't even realise it's there. This is the intended destination of an information security practitioner.

References

PCI DSS
https://www.pcisecuritystandards.org/security_standards/documents.php

TrueCrypt:
http://www.truecrypt.org/

Nmap:
http://nmap.org/download.html

WSUS:
http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx

Prepared by Encription Limited
www.encription.co.uk

+44 (0)330 100 2345

Email: enquries@encription.co.uk
Twitter: @encriptionit