Kick Your IT Security Up Seven Notches

MICHELL CONSULTING GROUP

www.michellgroup.com

Kick Your IT Security Up Seven Notches

IT Security. To some, it's pretty straight-forward cut-and-dry. To others, it's much more complex than that.

We definitely side with the latter.

One of the biggest mistakes companies make is taking a step or two for IT security, then forgetting about it – believing it's "handled". Very little could be further from the truth.

Could you imagine purchasing a robot babysitter, switching it on, and just trusting it to take care of your children while you're away? That seems ridiculous, but so many organizations simply purchase a security program, install it, and walk away. Granted, a business is not a child, but just like a child, a business must be raised, nurtured and protected.

When it comes to you children, you take every step possible to protect them. Do the same for your company. Here are seven ways you can do so.

29%

of SMBs used standard tools like configuration and patching to prevent security breaches in 2015

39%

of SMBs used standard tools like configuration and patching to prevent security breaches in 2014

— The Cisco 2016 Annual Security Report

1. Give Your Security a Safety Net – Or Better Yet, Several

As we've mentioned, one security measure in this modern age is simply insufficient. If you only have a single obstacle between the outside world and your network, chances are ridiculously good a hacker will find a way to slip past. And it's getting easier. The Cisco 2016 Annual Security Report showed that, in 2015, fewer SMBs (29%) used standard tools like configuration and patching to prevent security breaches than did the 39% who did so in 2014.

If you have to swing out on a trapeze, you're going to want multiple safety nets below you – in fact, the more, the better! It's the same for your IT security; you should have as many layers of security as you can manage. Very few things are more frustrating to a hacker than worming their way through your security – only to have another door slam in their face.

2. Keep Your Eyes Open

Multiple layers of security are awesome. But left alone, a determined hacker can potentially still find their way in. This is why keeping a close lookout is important.

A secure prison has walls, fences, barbed wire – many different layers of security. But still, they have guards posted in the watchtowers standing lookout. Watching over your network security is imperative to ensuring your secure system stays that way.

3. Lay Down the Law

According to IBM's 2014 Cyber Security Intelligence Index, a whopping 95% of ALL security incidents are instigated by human error. Ninety-five percent. That's enormous. It's equivalent to that prison we mentioned before having the walls, the fences, the barbed wire, AND the posted lookouts – and then one of the prison guard just forgets to lock the front gate.

Regardless of how much security you have in place – if you leave an opening for a cybercriminal to get in – they'll get in. Period. That's why it's absolutely critical to lay down rules and policies which will not only safeguard your network from within, they will also help to train your people for what to look out for and what not to neglect. Make sure that front gate is always locked.

95%

of ALL security incidents are intigated by human error according to IBM's 2014 Cyber Security Intelligence Index.

4. Slap a Patch on It

While we've reinforced it is not the "end all, be all," security software is absolutely an integral part of your network security. Typically, a strong security program will be able to carry the lion's share of the network security load, but again – there are ways around for a sneaky hacker.

One of the favorite ways hackers have of slipping in is to find and exploit a yet-to-be-discovered vulnerability in the program. The bad news is: once a hacker learns of this vulnerability, they will actively exploit it everywhere they can for as long as they can. They good news is: the software manufacturer is always on the hunt for these vulnerabilities and, as soon as one is discovered, they quickly create a free, downloadable patch to eliminate the vulnerability altogether.

However, no patch will ever benefit you if you never download and use it. Check for and download released patches on a regular basis.

5. Be Cryptic

After all the steps you've taken – from the security programs, to the training, to the lookouts, to the policies and patches – suppose after all that, you still manage to get hacked. Amazing as it sounds, practically nothing is utterly impossible in the world of cybercrime. After all the steps you've taken – from the security programs, to the training, to the lookouts, to the policies and patches – suppose after all that, you still manage to get hacked.

Amazing as it sounds, practically nothing is utterly impossible in the world of cybercrime. In fact, the 2016 Trustwave Global Security Report states that 97% of applications tested by Trustwave in 2015 contained at least one vulnerability.

But what then? Is your data just breached? You're now vulnerable? Not necessarily.

You can take measures to encrypt your data – or at least your most sensitive data – so that if it were to be made available to hacker, they wouldn't be able to make heads or tails of what they're looking at. Think of encryption as the last stand of your security – when all else fails and your data is taken, you're still fighting. At the end of the day, if you learn your data's been compromised but the encryption is keeping the data from being usable, you'll know your efforts were worthwhile.

6. Manage Your Passwords

"ilovemywife"
Sorry, your password must contain at least one digit.

"ilovemywife1"
Sorry, your password must contain at least one uppercase letter.

"Ilovemywife1"
Sorry, your password must contain at least one symbol.

"IloveMyFrigginWifeAWholeFrigginLotAndIHateThisStupidPasswordSecurityIWantToThrowMyFreakComputerOutTheWindowRightNow1!!!"
Congratulations! Your password is set. You'll enter this password every time you access the system.

This stinks. Nowadays, you're required to use ridiculously complex passwords – each one uniquely different from all your others – in order to ensure your account is secure.

But can YOU remember the password accepted above?

Of course not. Neither can you likely remember the multitude of other equally complex passwords you've had to select in your online life. That's how password management helps.

With password management, you can log into the program (ONE time with ONE password), and access all of your passwords – no matter how complex or weird they may be – in order to sign into your accounts. Having lots of complicated passwords can be hard. Luckily, password managers make it easy.

97%
of applications tested by Trustwave in 2015 **contained at least one vulnerability.**

7. Don’t just Delete – Super-Mega-ÜBER-Delete

We all know by now that simply highlighting a file and clicking “delete” doesn’t really delete the file. It simply moves it to a recycle bin, or a deleted files folder, or something similar. Then you have to re-delete it in order for it to be actually deleted.

. . . or is it?

Even going through these steps doesn’t guarantee your file is gone forever. Even if you format your hard drive and throw your computer away, someone could find it in a landfill and potentially still pull out your deleted files. The only real way – save from incinerating your hard drive into dust – is to utilize a deletion tool which is specially made to make files as irretrievable as possible.

Don’t just Be Secure – Be MCG Secure

As we’ve shown you, there are multiple (multiple, multiple, multiple) layers to strong IT Security – any and all of which Michell can provide for your organization. Don’t allow profiteers to destroy what you’ve worked so hard to accomplish. Protect it with all your might. Let’s talk about how we can secure your network with as many levels of security as you need.

MICHELL
CONSULTING GROUP

8240 NW 52nd Terrace Suite #410
Doral, FL 33166
305-592-5433
sales@michellgroup.com