TECHMinutes
September 2019
Your Small Business Technology Information Source!

This Issue:

Valuing Managed IT

It's difficult to put a value on your organization's technology solutions. While you might be tempted to assign a monetary value based on how much it all saves you, you also need to examine how much it costs you in the long term. Can you optimize your network even more than it currently is? Can you even keep track of the countless moving parts of your IT infrastructure? Managed IT might be able to help.

In the past, small businesses did everything they could to avoid IT maintenance, as they did not have in-house IT assistance available at...

Read the Rest Online!
https://dti.io/totwmanaged

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
newsletter.directive.com

Access Management Failings Keep Businesses Targeted

Your business' data is precious, and it goes without saying that there are plenty of entities out there that want to get their grubby little fingers all over it. This is especially the case these days, when credentials and remote access tools can be purchased on the black market and leveraged against organizations of all sizes. If you don't take action to keep your data secure from unauthorized access, you could face steep fines from compliance issues, not to mention the embarrassment of not being able to protect your organization's data.

Unauthorized Access?

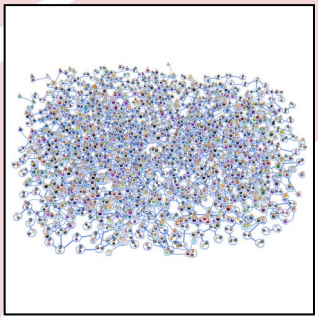
Anyone who has had their identity stolen (or have had an identity theft scare) knows how sketchy it can be. You might get an email saying that your account was accessed from an IP address in a country halfway across the world, during a time where there should be no one accessing that material. You immediately jump into damage control mode, changing passwords and kicking any unauthorized device off of the account, but it could be too late. In situations like this, there can be no doubt; someone has stolen your credentials and used them to legitimately access the account. What can you do to make sure this doesn't happen in the future?

Strong Passwords

Always use strong passwords. Don't use dictionary words or personally identifiable information in your passwords (like your mother's maiden name or your cat's name or your birthday). Instead, use a combination of random words, numbers, and symbols.

(Continued on page 2)

By Controlling Active Directory, You Can Control Your Whole Network



The protection of your business' computing assets is a bigger deal today than ever before. This is because there are dozens of ways that things could go wrong. One tool that many IT administrators like to use is called Active Directory, a feature found on most Microsoft Server operating systems that allow administrators to control users. This month, we take a look at Active Directory.

The first thing you should know about Active Directory is that there isn't a static plan that can be used by every business. We will go over some of the best practices, but you need to take into account that you need to configure your Active Directory settings to fit your business' needs. If your business is coming from a situation where it doesn't have any system in place, Active Directory is a great place to start.

Nobody Needs to be an Administrator

When someone logs into a business' domain server, they use their account, which by default is centralized in Active Directory. This alleviates the need for a central IT admin to log-in and set administrative privileges, and works across the network from the server to the endpoint to keep a business safe. After all, if people that don't need access to certain information, don't get access, nothing it lost. This is called **the least privilege administrative model.**

(Continued on page 3)

Your Business Could Use a Help Desk

If we asked you to imagine a world where your IT never suffered from technical issues related to your business' technology, would it feel too good to be true? Unfortunately, it's impossible for your organization to prevent every problem related to your IT. What is possible is for your business to encounter higher productivity and less downtime with the help of a dedicated help desk solution.

Businesses that have an in-house IT department that can act as a help desk have little to worry about; employees of these organizations know who to reach out to for their technology troubles. It's businesses that don't have access to IT resources that struggle with managing the day-to-day troubles of small business employees. Not everyone can afford to pay the salaries of multiple help desk technicians, leading some small businesses to tell their employees to deal with their issues themselves. This is a highly dangerous practice, and one that can lead to tasks being completed incorrectly.

Think about what could go wrong if one of your employees handles patching an operating system or mission-critical software solution, affecting their ability to get their work done. Even worse is the fact that some mistakes can potentially be so devastating that entire workdays can be wasted trying to resolve a problem that shouldn't even be a problem in the first place. Compare this situation to what would happen if the employee had a dedicated IT professional to turn to for any questions or concerns regarding their technology and you'll notice a stark contrast.

When you outsource your help desk solution, you gain all of the benefits of having an in-house help desk without actually having them on site. We live in a day and age where technology support can be provided remotely without the need for an on-site visit.

Furthermore, if you provide your employees with a single point of contact for all of their technology needs, suddenly all of the excuses for not getting any work done due to technology troubles disappear, meaning you can rest assured that IT issues are addressed properly with minimal downtime associated with them.

Directive can help you implement the ideal help desk solution--one that works for your business and actively seeks to prevent small addressable issues from becoming major time sinks or costly problems. To learn more, reach out to us at 607.433.2200.

Share this Article!
https://dti.io/useahd

Access Management Failings Keep Businesses Targeted

(Continued from page 1)

More importantly, don't use the same password across multiple accounts. If you sign into a fishing enthusiasts forum with the same password you use for PayPal, you are putting both accounts at risk.

Two-Factor Authentication

Two-factor authentication is a great way to keep your data secure. In this particular case, you're essentially adding an additional layer of security to your accounts. Instead of just needing a username and password, you need access to another device associated with the account that receives a passcode. In this way, you effectively keep hackers from accessing your account without also having access to your secondary device.

Remote Monitoring

We believe that access control is especially important for business environments, and to that end, we offer a comprehensive remote monitoring solution that gives us insights into who is accessing your network, from where, and when. By utilizing this tool, we can limit access to sensitive data, detect when there is a security breach, and take measures to mitigate the damage done by such an event.

Of course, this only helps to keep outsiders from accessing your sensitive data. What if an insider is accessing information they aren't supposed to see? In this case, we recommend putting together a list of permissions for each user based on their role within your organization. Nobody needs access to every single bit of data that your business utilizes, except maybe executive leadership. A good rule to live by is this: The less data that an employee has access to, the better your security. This isn't to say that you should deprive employees of information that would make their jobs easier; rather, you instead protect data by restricting access to those who need it during their day-to-day responsibilities.

What's At Stake

You don't need us to tell you that unauthorized access to sensitive data is a bad thing, but often times businesses might not get why it's such a big deal. Specific industries might be subject to regulations that define standards for security, and the last thing these organizations can afford is the gratuitous fine associated with failing to do so. Furthermore, your business' reputation will be at stake. You may have heard the phrase, "Bad publicity is still publicity," but we assure you that in this case, it's simply not how it works.

If your business falls victim to a hacking attack, imagine the outrage that your local news outlet will throw your way...

Read the Rest Online!
https://dti.io/failtarget

By Controlling Active Directory, You Can Control Your Whole Network

(Continued from page 1)

It works like this: each user has the minimum permissions to complete their work. You can always elevate access temporarily if needed. Otherwise, if a user gets a virus, that virus will have the same access the user does, and could do a lot more damage because the user has access he or she didn't need in the first place. The virus has the capability to spread across the network, where if the user's permissions were locked down, the virus would only have a minimal impact.

This means that everyone on the network, including the business owner, the employees and the IT staff log in as a regular non-administrator to do their normal day-to-day work. If they need to get administrative control, they can log in with a separate admin account. You will want to keep credentials to that administrative account safe and protected.

Force Strong, Complex Passwords and Set Password Expirations

Most people aren't able to memorize complex passwords. Some can't even create them. Unfortunately for everyone, the people that want to break into computing networks have tools that are extremely proficient at guessing passwords that aren't complex enough.

You will want to ensure that your staff has learned the value of the use of a passphrase. Instead of combining string of words that could potentially makes sense, stringing together multiple random words is actually more secure. Keep in mind, the words need to be very random. Here's a quick example:

Bad Passphrase Examples:
1worldtr@decenter
n0diggityn0doubt
c0ttag3ch33s3
Decemberse7en1941
ilovepizzawithmushoom$

Good Passphrase Examples:
Dd3sk0fm1ght33meatba#
Pr04ac1v3h3rbp0ss3
GREENbottletabletra
3@ster1sn0samureye

Back to Active Directory, you should require passwords to be long - at least 12 characters, and settings should lock a user out after three failed attempts. Forcing passwords to expire every month or two is a good strategy to ensure that password security is maintained.

Delegate Permissions to Security Groups, not Individual Accounts

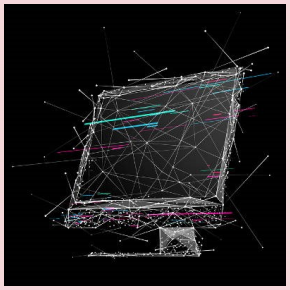
When we go in and audit a new prospect's network, we often find that they have gone ahead and assigned permissions to individual accounts rather than using security groups. As your organization grows this can present problems with controlling access. Keeping track of who can see what using security groups is a much better and more organized option.

Use LAPS (Local Administrator Password Solution)

Inside Active Directory, there is a...

Read the Rest Online!
https://dti.io/activecontrol

Protect Your Computing Infrastructure with Remote Monitoring and Management



Some businesses struggle with finding the right technology management support. There are several factors that come into play, including physical location of the service provider, distance to and from the worksite, and ease of support. In fact, managed IT services are one way you can sidestep the difficulty of finding access to affordable technology support entirely through the use of remote monitoring, maintenance, and management.

Remote Monitoring

Businesses need someone out there monitoring their networks for inefficiencies and security threats. With remote monitoring, your business can focus on getting work done without worrying about whether or not your infrastructure is working in the best way possible. Remote monitoring is particularly helpful for detecting issues early on before they are affecting operations, meaning they can be addressed before they become downtime-inducing problems.

Remote Maintenance

Visits to the office are fine and all, when your organization isn't suffering from operational inefficiencies. There is a reason why many businesses have opted into remote maintenance, which makes the odds of waiting around for maintenance much lower. Keeping your hardware and network running effectively often is a way to keep your business running effectively. Maintaining software systems and patching hardware as needed are all parts of a conscientious remote monitoring strategy.

Remote Management

Most issues regarding your business' IT infrastructure can be resolved without an on-site visit, and with remote technology assistance at an all-time high, you can bet that it's an efficient way to handle this aspect of your business' technology. With the right configurations and setup, technicians can remote into your organization's infrastructure and tweak things as needed, all without an on-site visit.

Directive can help your organization discover new and exciting ways to make your technology infrastructure work for you.

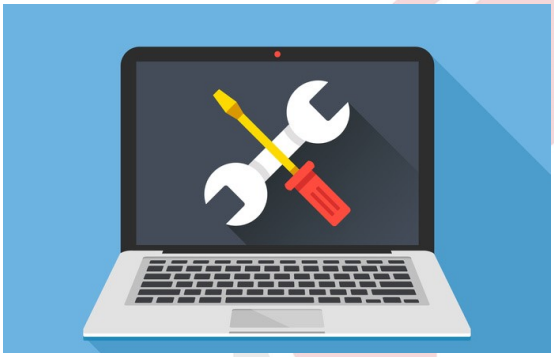
To learn more, reach out to the IT experts at 607.433.2200.

Share this Article!
https://dti.io/protectrmm

Alert: Microsoft is Retiring Two Major Operating Systems

Windows is a great operating system, but unless you're keeping track of which version you have, you'll be in for a rude awakening when it comes time to upgrade. In just six short months, there will be two Windows End of Life events for major technology solutions: Windows 7 and Windows Server 2008 R2. You need to start thinking about upgrading now before it's too late to do so.

The End of Support date for these two titles is January 14th, 2020. If your organization hasn't already upgraded away from these solutions, or has yet to take steps toward doing so, you should seriously consider doing so soon. A full migration cannot be done overnight, and vulnerabilities could appear in the time you're spending trying to upgrade away from these pieces of software.



This is why we recommend you start thinking about it now; your security is at stake, and by extension, your business' future.

Windows 7

Even though we are currently on Windows 10, Windows 7 has been a remarkably popular operating system since its inception many years ago. In fact, it wasn't until just this past December that Windows 10 overtook Windows 7 in number of users. There is currently an ongoing campaign running to get Windows 7 users to make the upgrade as soon as possible.

We recommend making the jump to Windows 10, as it is the most recent operating system supported by Microsoft. If you need to move over several workstations to this operating system, the process might be slow-going, which is why we recommend starting talks to make this happen now. We are of the firm belief that working with consultants can make this process go as smoothly as possible.

You could also go the Microsoft 365 route, which is a cloud-based service for companies that may not be able to afford to cover the initial costs of upgrading to Windows 10. Directive can help you make the decision regarding which service is appropriate for your business.

Windows Server 2008 R2

Microsoft is also ending support for Windows Server 2008 R2, meaning that any business that relies on it for data and application hosting will be out of luck come January 2020. This is particularly notable for any server infrastructure you may have that utilizes Windows Server 2008 R2, as it will no longer be receiving security updates that are critical to keeping your data safe.

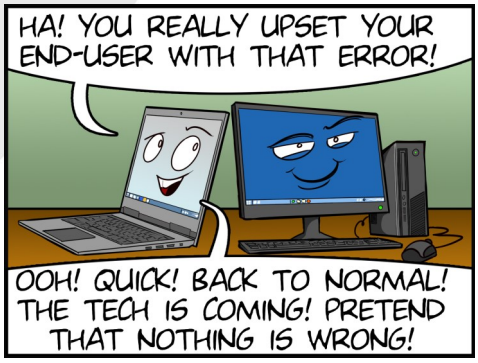
There are two new versions of the Windows Server software that you could upgrade to, as well as the cloud-based Azure platform. With the right tools and upgrade procedure, you might be able to save some money when you make the jump to a more recent OS. For more information on how to make this happen with minimal downtime and risk, consult the IT professionals at Directive. You can reach us at 607.433.2200.

Share this Article!
https://dti.io/2ostoretire

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Chris Chase
Solutions Integrator

Charlotte Chase
Solutions Integrator



Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com
facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com
instagram.directive.com