SentinelIPS

Security by the Seasons:

Tying upgrades and updates to the calendar makes the mundane tasks manageable

Managed Intrusion Prevention with 24/7 monitoring and stellar support.
Intrusion Prevention is never simple, but we make it simple for you.

Visit us today at
sentinelips.com

- ✓ CINS ACTIVE THREAT INTELLIGENCE
- ✓ NETWORK VISIBILITY
- ✓ STOP MALWARE AND RANSOMWARE

A business' data network is a living thing. It's always active, always moving. And responding to the needs of the network and the people who use it on a daily basis is a full-time job all by itself.

But just like any other living thing, a network needs regular maintenance if it's going to perform optimally. Far too often IT staffs, particularly at smaller companies, are too small to dedicate one person to just one job. Instead, they are taking a staff — sometimes made up of just a single employee — and stretching it thin in an effort to deal with the daily emergencies that will no doubt occur. That leaves no time for the updates to software, the upgrades to hardware, and the training of people that's needed to keep a network safe and data protected.

How can those upgrades and updates still happen without increasing staff or taking days or weeks that a single employee doesn't have to dedicate to the task? By doing them seasonally.

Dividing the data center into four broad categories — hardware, software, network and data — and assigning each of those categories a season makes the process of routine maintenance manageable.

Here's how we'd do it.

Spring:

Get a Handle on Your Hardware

If you've developed blinders to the tangle of multi-colored cords sprouting from the back of your server racks, you aren't alone. Do a web search for "server room from hell" and you'll see plenty of examples that are probably worse than yours.

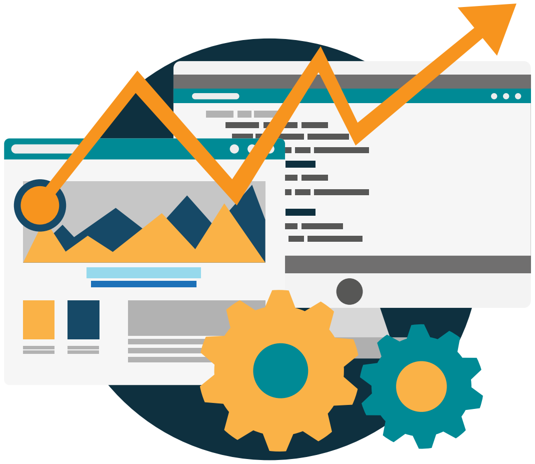
And it's not just time-strapped staffs that struggle with keeping hardware current. Even the team at CERN that operates the large hadron collider finds it tough. When the organization decided it was time for large-scale improvements to its most powerful piece of equipment, engineers in Geneva had to do some prep work first. Included in that was removing some unused cables from the system. How many? 9,000.

It's an astounding number, but how they got there is probably pretty familiar. Over the years, as improvements and upgrades were made to individual parts of the collider, the cables that were initially installed were also replaced, but the old cables weren't removed.

Obviously, that's an extreme example, but we all know it's easy to lose the handle on your hardware. That's why it's important to take some time each spring to make sure you don't. Here are three things you need to do.

Refresh Your Network Diagram

If the photos that pop up when you enter "server room from hell" into a search engine don't scare you then it's definitely time to take this step. Even if you are horrified, it's still time for a fresh network diagram, because yours is almost certainly out of date.



Keep in mind that you're worried about more than just organization. You need to be sure there still isn't some test box receiving a tap of all of your network traffic from a mirrored port on a switch somewhere. So, take the time to do a thorough audit of each Ethernet port and wireless access point, know where those cables lead, and evaluate the necessity of each piece of equipment. Why? Because each device you have connected to the network is another opportunity for hackers to move throughout your network and another home for malware to live.

Know What’s Normal

To know when something is wrong on your network you have to know what normal traffic looks like. What machines should be talking to each other? How often should they be talking? What ports should they be using? Put some network monitoring software in place so you know what to expect, and review that data regularly. Anomalies could be a clear sign of an infection or breach.

Is Your Bandwidth Able to Handle Your traffic?

While data centers at larger companies may have gotten there a few years ago, a lot of SMB networks are finally making the move to 10 Gbps internal switches and infrastructure, and 1Gb+ speeds are becoming more commonplace on gateway connections, as well. Is your bandwidth up to snuff? Are you prepared to handle data moving at those speeds? If not, perhaps it’s time to consider upgrades to your hardware.

Summer:

Don't Let Your People Be Your Problem

The weakest part of any network isn't some tool in the data center or some device on the wire. No, it's the people who are logging in.

Whether it's the employee in the British Office of Communications who downloaded years worth of broadcaster data to take to a new employer or it's the regional manger at a beauty supply chain who was a little too lazy with a password, most data breaches occur by someone logging into the network legitimately.

Either through intentional misdeeds or ignorant mistakes, your people are the biggest threat to your network. And while you can't necessarily control what an angry soon-to-be-ex employee does, you can do your best to control the damage any employee can do, malicious motives or not.

Actively Manage User Accounts

If you're using Active Directory, use the auditing feature to review user accounts and privileges, logon activity, and account policies. This is how you can make sure that employees aren't nosing around areas of the network they shouldn't be or downloading files that they shouldn't have access to.

Also use the auditing feature to look for old or redundant accounts and remove them.

Audit All Systems

This really does mean all. You want to look at your internal systems, everything from an intranet to custom applications. You also want to look at anything that's external, like an Amazon AWS account or other managed service accessed through a browser. What are you looking for? Again, old or inactive accounts. Get rid of them. Also check to make sure that the people who have access to these systems are still supposed to have access. Someone may still be an employee but in a new role and access may no longer be necessary.

Review Authentication Systems

Your people need secure passwords. That’s a given. But do your authentication systems allow them to make truly secure passwords? And do your people even know what that means? It’s not about cute combinations of letters, numbers and special characters like we’ve been teaching them for so long. Those passwords aren’t that strong when put up against rainbow tables and sophisticated brute force hacking techniques.

Passwords made up of a combination of three or four random words are infinitely easier for your people to remember and exponentially harder to crack, but too many authentication systems aren’t prepared to handle a password like that. Use one that is.

Consider User Management Software

This would be in addition to Active Directory. Software like Okta or Centrify can provide an extra layer of protection against stolen credentials or an identity-based data breach.

Train your people

You can put measures in place. You can keep directories and user lists updated. Still, the best way to make sure your people aren’t a liability is to make sure they are regularly trained. Hackers are always updating their methods. Your people need to be kept up to date on what social engineering techniques they might see.

There are some great third-party resources if this training isn’t something you have the capacity to handle in-house or it’s something you aren’t comfortable doing on your own. One to consider: Securing the Human by the SANS Institute. It’s thorough; it’s customizable; and it can all be done online.

Fall:

Get to Know Your Network

If your server room is like most others, somewhere in a back corner there's a box that has been plugged into the switch since no one knows when. Another thing that no one knows: what that box actually does.

So, as part of the fall clean up, dive in. Figure out what the box does and then yank the power cable if you don't need it anymore.

What other networking tasks should you take on? Here are four.

Take Inventory of Your Equipment

While you're looking at the network diagram to figure out what that mystery box does, take a few minutes to do a physical inventory of your equipment. Anything missing?
Anything need replacing?

You have to know what you own. You have to know how old the equipment is and when it needs to be replaced. And speaking of replaced, does anything need to be swapped out now? Be proactive about making sure that your critical systems are kept up to date. Better to do it now than when you are forced to do it in a crisis. You'll save money, time, and resources in the long run.

Take Inventory of Your Software

And while you're in audit mode, look at your software too. It's important to know what's on your system for purposes of license renewals, policy decisions, and network security concerns.

Do a Companywide Audit of Your Patches

Chances are you’re already on top of regularly patching your systems, but an annual check to make sure nothing has been missed is a precaution worth taking. This is especially true if you have a lot of transient assets — laptops, tablets and phones that move in and out of the network. It’s too easy for those to get left in a bag or a pocket and a critical update be missed, leaving either the device operating inefficiently or, more important, the network vulnerable when it doesn’t need to be.

Is it Time to Outsource?

This list of network tasks isn’t long, but that doesn’t mean it’s easy either. Audits like the kind we are talking about here are time consuming. For IT departments that consist of one or two people, being able to set aside time to do this kind of necessary work is tough. For some, it’s impossible. If that’s the case, have you considered outsourcing some or all of your network management?

There are definitely some network devices that you can have managed remotely. We can think of at least one security device. There are also some Software as a Service solutions you might want to consider. Your people could be operating with the latest versions of, let’s say, their accounting software of choice and you aren’t having to manage licensing or updates.

Granted, budgeting can be an issue when it comes to outsourcing, but it’s always something worth considering.

Winter:

Don’t Forget About your Data

Having the right hardware is important. Software too. And you know how we feel about the importance of training your people. But the heart of any business is its data. For some businesses, it helps them get products to market faster. For other businesses, the data is the product.

Keeping that data safe and accessible by the people who have a legitimate right to it and need for it is why so much research is put into buying the right hardware, the right software, and the right training for your people. But that data doesn’t just need to be safe and accessible, it also needs to be up to date. That’s why it also needs to be part of what you look at while you’re doing your seasonal security clean.

So, what do you need to do to keep your data updated? Here are five ideas.

Review Your File Shares

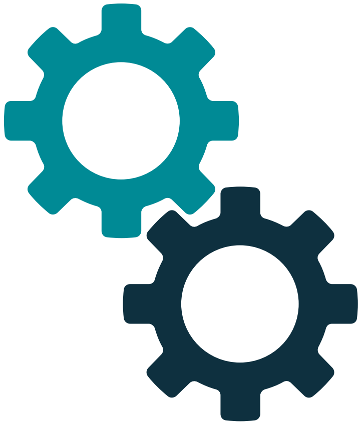
The shared data directories on file servers are a cesspool of old and irrelevant data that’s wide open for ransomware infection. It doesn’t have to be. Review file usage and remove unnecessary clutter. Reorganize the folders system then review and update user and access permissions, that way once you get the data in order only the people who need it can get to it.

Ensure File Server Patches are Updated

We mentioned this when we talked about your network, but it’s important to make sure that all of your file servers have the latest patches and updates made to them. Not only that, vulnerability scans need to be run regularly and any deficiencies that are found need to be addressed.

Check and Update Your Backups

Your backups need to not only be running smoothly but they need to include any new servers and their data. It's also a good time to check and make sure that you exclude any servers that don't exist anymore. Also, timely, accurate backups are a critical step in the fight against ransomware.



Make Time for General Database Maintenance

Databases need maintenance, too. For example, review your postgresql database procedures to ensure the databases are vacuumed properly and running smoothly. Improving this aspect of your database systems could have a significant impact on your internal systems' performance.

Consider Outsourcing

We asked it before, and we'll ask it again. Is data management like this something you should outsource? It's a lot of work, and chances are your staff is small. A budget-friendly way to get the kind of data management you need without adding responsibility to an already over-burdened staff is by turning to the cloud. Cloud-based data warehousing and Database as a Service offerings are growing both in popularity and quality.

We've put these tasks in seasonal order, but, honestly, there's nothing that links any of these tasks to a specific season. While they are all important, they can be done at any time. So, take a look at your own network. Decide what you need to tackle first, and start there. Then take the remaining tasks and find the right season for those. For example, the audits we describe in the section on the network can require some time. Maybe there's a period in your year that is unusually slow. Plan to tackle those then.

But tackling is the important thing. All of these tasks need to be done. None of them can slip. Even if you don't use our seasonal method, make sure you find the time for them in your schedule.

Sign up for Sentinel IPS or simply learn more by visiting www.sentinelips.com