ASLAN COMPUTER SYSTEMS

2015-03 EVERGREENING

Evergreening

Evergreening is the practice of replacing technology and computing devices on a scheduled plan. Aslan Computer Systems recommends replacing workstations on a 3 year cycle and servers every 3 to 5 years. Adopting this approach involves replacing about one third of workstations each year. A server replacement plan can be established based on the number of servers involved and the replacement cycle. Aslan recommends that any server or critical workstation that is out of warranty be strongly considered for replacement.

Benefits

An evergreening policy will provide stable and reliable computer servers and workstations to employees who require them. Specifically, it:

- Allows replacement of computers on a planned basis.
- Allows budgeting for replacement.
- Spreads replacement costs relatively evenly across years.
- Supports tax planning by aligning with the practice of depreciating computers over three years.

- Helps ensure that hardware is always under warranty when warranties are purchased to match the planned life cycle of the system (eg. 3 years for workstations and 3-5 years for servers).

Getting Started

Organizations that are adopting an evergreening strategy/policy need to transition from their current practices. One way to transition is to replace the oldest one third of workstations in the first year, the second oldest one third in the second year, and the remaining workstations in the third year. At the end of three years, the oldest workstations will be not more than three years old.Aslan Computer Systems can help clients by identifying workstation replacement candidates and facilitating creation of a server replacement plan. Call us for more information...

Tips and Tricks

Sometimes the keyboard is faster than the mouse. Try these program key combinations:

CTRL+C:	Copy	CTRL+B:	Bold
CTRL+X:	Cut	CTRL+U:	Underline
CTRL+V:	Paste	CTRL+I:	Italic
CTRL+Z:	Undo		

Security Trends

Viruses are more prevalent than ever... In their webinar “2015 Security Trends”, Watchguard Technologies observed the following regarding 2014: “The total number of security incidents detected by respondents climbed to 42.8 million this year, and increase of 48% over 2013. That’s the equivalent of 117,339 incoming attacks per day, every day.” If you travel, thirdcertainty.com says that you can protect yourself if you:

- Watch for fake Access Points â€“ they use default names that manufacturers use like dlink, cisco, netgear or trusted names like ShawOpen, AT&T Wi-Fi, and Free WiFi, and can capture private information by logging keystrokes.
- Don't connect to an open network (one that doesn't require any password or have security settings).
- Use a VPN for connecting – a VPN will help you encrypt everything you can.
- Check the Wi-Fi settings and look for the list of accesspoints you have connected to â€“ prune the list down to remove any that you don't connect to regularly. (From the Windows menu, type "Manage Wireless Networks", Click on "Manage Wireless Networks" in the search result. This will bring up the list of wireless networks to prune.)

For more, see http://thirdcertainty.com/best-practices/hazards-using-public-wifi-access-points/

Wikipedia Definition for Malware: short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.Aslan can help you find the right combination of antivirus, antispam, and firewall solutions to meet your security needs and budget. Call us at 780-437-9504.

New Technology

The Internet of Things (IoT) is a hot topic these days. But what is it, what does it mean to you, and what are the risks?

Traditionally the Internet has been used to provide access to information (via a browser) or to people (via an email). But now more and more 'smart' things are connecting, like smart phones, programmable thermostats, smart TVs, programmable appliances, tablets, game consoles, garage door openers and many others.

Anything that you connect to your WiFi or plug into your network is a potential entry point to personal data on computers in the home or office. So now we have people to people, people to things, and things to things connections.

The IoT can help you:

- Check on your baby

- Remember your meds
- Track your workout activity
- Find your keys
- Find a vacant parking spot
- Keep track of your assets (things)
- Make sure the oven is off or the lights are on
- Turn down the crock pot if you are going to be late, but it can't help you take the food out of the fridge and put it in the crock pot (yet).

It can help government and industry:

- Know when garbage containers are full
- Track electricity usage
- Schedule maintenance before equipment breaks
- Monitor pollution
- Track water flow, lion movement, or illegal log movement
- Upgrade your software

If you choose, it allows Aslan to:

- Track the health of your computers
- Receive notifications when computers or networks fail, even before you know there is a problem
- Set up printer services to deliver toner before your printer runs out

CMS Wire reports security and privacy concerns with a set of IoT devices they tested. Some of the tested devices:

- Collected some personal information
- Failed to require strong passwords
- Had Web User Interface security concerns
- Used unencrypted communications between devices and for software updates

Essentially your non secure items that are accessing the internet can be a gateway to the rest of your network. This highlights the need for increased network security at home and in the workplace. Increased perimeter security (ie. firewall or router) can help to protect against this.

Aslan can provide firewalls, routers and services to keep you properly protected against vulnerabilities introduced by insecure IoT items.

Sources:

http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

http://postscapes.com/internet-of-things-examples/

http://www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php

Q & A

Question:	I have antivirus software, why do I get viruses and malware?
Short Answer:	Because the viruses and malware are designed to try and get around antivirus software.

For more, see https://askleo.com/i_run_antivirus_software_why_do_i_still_sometimes_get_infected/

If you think someone you know would appreciate and benefit from this information, please forward it to them or SHARE it on:

If you received this from someone you know, and would like to see it on a regular basis, please subscribe or FOLLOW us on: