Computer virus and world wide web

Technology, Computer

Workstation and desktop devices are prone to viruses, mallard, and malicious software, especially If the user surfs the Internet and World Wide Web. Given that users connect to the Internet and World Wide Web, what security countermeasures can organizations Implement to help mitigate the risk from viruses, mallard, and malicious software? Organizations can restrict specific sites, key words like blobs, mirror sites and such. Organizations can also make sure specific ports are shut down; this can prevent back doors when accessing a site.

There are a lot of web sites out there that o not need accessibility, especially for a work environment. 2. Your employees e- mail file attachments to each other and externally through the organization's firewall and Internet connection. What security countermeasures can you implement to help mitigate the risk of rouge e-mail attachments and URL Web links? The basic step would be to not allow hyperlinks to automatically work when In an e-mail. Some times when a link Is In a user can click and It will automatically launch It. Another step would be for the e-mail to have the user's signature.

This Is usually overruled through the user's machine, for example In the military we have a Common Access Card. This card is a form of identification on multiple levels, in order for you to access your e-mail you need to log in with your CA and enter your pin. When you send an -mail it has a signature on it based on the code in your CA, this way the person receiving the e-mail knows it is from you. Another way of doing it is by having public keys and private keys, this way both users know it is from the individual. 3. Why is it recommended to do an antivirus signature file update before reforming an antivirus scan on your computer?

From what the lab showed me and from my understanding it is because the scan will not scan encrypted files. The signature file would have been able to pick It up and It would work In tangent with the scan. 4. Once a malicious file is found on your computer, what are the default settings for USB/removable device scanning? What should organizations do regarding use of USB hard drives and slots on existing computers and devices? Some devices have serial numbers associated with them, and this string is optional. This is defaulted with thumb drives, USB hard drives and Pads.

Most scanning and tracking details would be of most use with the USB mass storage devices. Organizations should immediately remove the AUTO run feature! This is basic in the military, any one would be able to come In and throw a thumb drive and automatically run whatever it is on It making it a vulnerability. 5. If you find a suspect executable and wish to perform " dynamic analysis" what does that mean? Dynamic analysis Is the testing and evaluation of a program by executing data in real-time. The objective is to find errors in a program while it is and malicious code sandbox?

This can be potentially dangerous but it is looked like as a sandbox. This is by running the virus, preferably in a machine with limited access to a network and something that isn't much of a use and executing the virus in real time. This way you can debug the virus and see what is it doing so you can detected and prevent it. 7. What are typical indicators that your computer system is compromised? It is slow, everything you do takes a lot longer to perform. You are missing data, our peripherals are not responding or they are performing automatic actions.

Your computer starts up during odd hours and it is used as a zombie computer. You have additional items on your browser, you have an entirely different browsers, items are opening up and there are a lot of pop ups. 8. Where does BAG Business Edition 2012 place viruses, Trojan, worms, and other malicious software when it finds them? According to the lab it is quarantined, it is isolated and then removed by the user's request. I am assuming it is then directed to the BAG corporations for further analysis fir updates.