10 things you should do to secure every general-purpose operating system

Version 1.0
November 13, 2007

This information is based on the IT Security blog post "10 security tips for all general-purpose OSes," by Chad Perrin.

There are key considerations for system security that apply no matter which general-purpose operating system platform you happen to be using. You should always consider the following precautions when securing your systems against unauthorized access and unfortunate disasters.

1 Use strong passwords

One of the simplest ways to improve security is to use a password that isn't easily guessed by brute force attacks. A brute force attack is one where the attacker uses an automated system to guess passwords as quickly as possible, hoping to find the right password before long. Passwords that include special characters and spaces, numbers, and both capital and lowercase letters—as well as avoiding words in the dictionary—are much more difficult to crack than your mother's name or your anniversary date.

Remember as well that increasing the length of your password by just one character multiplies the total number of possibilities by the number of valid characters that can be used. In general, anything fewer than eight characters is considered far too easy to crack. Ten, 12, or even 16 is better. Just don't make it too long to remember or too difficult to type.

2 Invest in good perimeter defense

Not all security occurs on the desktop. It's a good idea to use an external firewall/router to help protect your computer, even if you have only one computer. At the low end, you can purchase a retail router device, such as the commercial Linksys, D-Link, and Netgear routers that are available in stores such as Best Buy, Circuit City, and CompUSA. Higher up the scale, you can get managed switches, routers, and firewalls from "enterprise-class" vendors, such as Cisco, Vyatta, and Foundry Networks.

Starting somewhere in the middle and moving all the way up to direct competition with the major enterprise-class vendors, you can put together your own firewalls either from scratch or using prepackaged firewall/router installers, such as m0n0wall and IPCop. Proxy servers, antivirus gateways, and spam filtering gateways can all contribute to stronger perimeter security as well. Remember that in general, switches are better for security than hubs, routers with NAT are better than switches, and firewalls are a definite necessity.

3 Update your software

While concerns such as patch testing before deployment to production systems may be of critical importance in many circumstances, ultimately, security patches must be rolled out to your systems. Ignoring security updates for too long can result in the computers you use becoming easy targets for unscrupulous security crackers. Don't let the software installed on your computers fall too far behind the security update schedule. The same applies to any signature-based malware protection software, such as antivirus applications (if your system needs them), which can't be any more effective than the degree to which they are kept up to date with current malware signature definitions.

4 Shut down services you don't use

Often, computer users don't even know which network-accessible services are running on their systems. Telnet and FTP are common offenders that should be shut down on computers where they are not needed. Make sure you're aware of every single service running on your computer and have a reason for it to be running. In some cases, this may require reading up on the importance of that service to your particular needs so that you don't make a mistake like shutting off the RPC service on a Microsoft Windows machine and disallow logging in, but it's always a good idea not to run services you don't actually use.

5 Employ data encryption

Varying levels of data encryption coverage are available to the security-conscious computer user or sysadmin, and choosing the right level of encryption for your needs is something that must be decided based on circumstances. Data encryption can range from use of cryptographic tools on a file-by-file basis, through filesystem encryption, up to full disk encryption.

Typically, this doesn't cover the boot partition, as that would require decryption assistance from specialized hardware, but if your need for privacy is great enough to justify the expense, it's possible to get such whole-system encryption. For anything short of boot partition encryption, a number of solutions are available for each level of encryption desired, including both commercial proprietary systems and open source systems for full disk encryption on every major desktop operating system.

6 Protect your data with backups

One of the most important ways you can protect yourself from disaster is to back up your data. Strategies for data redundancy can range from something as simple and rudimentary as periodically saving copies to CD to complex, staggered, periodic automated backups to a server. On systems that must maintain constant uptime without loss of service, RAID can provide automatic failover redundancy in case of a disk failure. Free backup tools, such as rsync and Bacula, are available for putting together automated backup schemes.

Version control systems, such as Subversion, can provide flexible data management so that you can not only have backups on another computer, but you can keep more than one desktop or laptop system up to date with the same data without a great deal of difficulty. Using Subversion in this manner saved my bacon in 2004 when my working laptop suffered a catastrophic drive failure, emphasizing the importance of regular backups of critical data.

7 Encrypt sensitive communications

Cryptographic systems for protecting communications from eavesdroppers are surprisingly common. Software supporting OpenPGP for e-mail, the Off The Record plug-ins for IM clients, encrypted tunnel software for sustained communication using secure protocols such as SSH and SSL, and numerous other tools can be had easily to ensure that data is not compromised in transit. In person-to-person communications, of course, it can sometimes be difficult to convince the other participant to use encryption software, but sometimes that protection is of critical importance.

8 Don't trust foreign networks

This is especially important on open wireless networks, such as at your local coffee shop. If you're careful and smart about security, there's no reason you can't use a wireless network at a coffee shop or some other untrusted foreign network, but the key is that you have to ensure security through your own system and not trust the foreign network to be safe from malicious security crackers. For instance, it is much more critical that you protect sensitive communications with encryption on an open wireless network, including when connecting to Web sites where you use a login session cookie to automate authentication or enter a username and password.

Less obviously, make sure you don't have any network services running that are not strictly necessary, as they can be exploited if there is an unpatched vulnerability. This applies to network filesystem software, such as NFS or Microsoft CIFS, SSH servers, Active Directory services, and any of a number of other possibilities. Check your systems both from the inside and the outside to determine what opportunities malicious security crackers may have to compromise your computer and make sure those points of entry are as locked down as reasonably possible.

In some respects, this is just an extension of the points about shutting down unneeded services and encrypting sensitive communications, except that in dealing with foreign networks, you must be especially stingy with the services you allow to run on your system and what communications you consider "sensitive." Protecting yourself on a foreign, untrusted network may in fact require a complete reworking of your system's security profile.

9 Get an uninterruptible power supply

You don't just want a UPS so you won't lose files if the power goes out. There are other, ultimately more important reasons, such as power conditioning and avoiding filesystem corruption. For this reason, make sure you get something that works with your operating system to notify it when it needs to shut itself down, in case you aren't home when the power goes out, and make sure you get a UPS that provides power conditioning as well as battery backup. A surge protector simply isn't enough to protect your system against damage from "dirty" power. Remember, a UPS is key to protecting both your hardware and your data.

10 Monitor systems for security threats and breaches

Never assume that just because you've gone through a checklist of security preparations your systems are necessarily safe from security crackers. You should always institute some kind of monitoring routine to ensure that suspicious events come to your attention quickly and allow you to follow up on what may be security breaches or threats to security. This sort of attention should not only be spent on network monitoring but also integrity auditing and/or other local system security monitoring techniques.

Other security precautions may apply depending on the specific OS you use. Some operating systems provide additional security challenges because of design characteristics that produce a less-than-optimal security profile, and some operating systems grant the knowledgeable sysadmin capabilities for increased security that may not exist elsewhere. You should keep all of this in mind when securing your system, whether using proprietary systems, such as Microsoft Windows and Apple Mac OS X, or open source systems, such as your favorite Linux distribution, FreeBSD, NetBSD, or even the security-conscious OpenBSD.

Only in the rarest of circumstances is a default install of your OS, with no further thought to securing the system, truly sufficient. Start with the above enumerated security concerns regardless of your operating system and then consider the specific security needs and opportunities of your platform. Don't leave the integrity of your system's security up to luck.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for TechRepublic's Downloads Weekly Update newsletter
- Sign up for our IT Security NetNote
- Check out all of TechRepublic's free newsletters
- Windows XP services that can be disabled
- Take charge of Windows XP with these 10+ power tips
- 10 free security tools you should already be using

Version history

Version: 1.0
Published: December 13, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team