by the Trey Internet team and Lee Kimber, Microsoft Program Manager

Download a printable version of this column: **ISP Security Practices List** *(55 KB - .doc file)*

Security is as much about policing and good practice as it is about using secure products. Internet service providers (ISPs) are on the cutting edge of developing security practice because their operations rely on exposing systems and services in a way that most companies do not.

From remote access server (RAS) terminals to Web servers, ISPs expose different services on different hardware to different users whose connection, access, and usage rights must all be set, authenticated, and enforced.

To discover best practices for managing and policing all these variables, Microsoft Service Providers asked Trey Internet (we've changed their name and distinguishing information to protect them) to detail the security checklist they use for their all-Windows platform. This list separates actions by their frequency--some actions are constant; others are performed daily, weekly, or monthly. Use the checkboxes to compare your security practice with Trey Internet's recommendations.

Operating System Security

Constant

□ **Limit user rights so they don't have more power than is necessary.**
Create users as standard users. Then remove Terminal Services client rights, and add remote access server (RAS) rights.

□ **Limit any window for vulnerabilities that can be exploited when bringing up new servers.**
Bring up machines on the network with Remote Installation Services (RIS) and preconfigured images with necessary patches installed.

□ **Limit Terminal Services access to the smallest number of accounts possible.**
Only administrators of your ISP should have Terminal Services access.

□ **Run a two-tier DNS structure to protect the identity of internal servers.**
Such a system involves running four DNS servers, two of which are visible to the outside world and two of which are hidden behind the firewall. The two external DNS servers do not query or reference the two internal DNS servers. The external DNS servers only handle records for the mail and Web servers. The two internal DNS servers handle all Active Directory® requests. They host the Active Directory-enabled domain of the ISP and its reverse-lookup zone. They are blocked from the Internet at the firewall level. The internal servers forward DNS requests that they cannot service themselves to the two external DNS servers.

Note: Trey Internet does secondary replication of some zones between the internal and external DNS servers. This is for administration and includes zones like inaddr.arpa.

□ **Run an Intrusion Detection System (IDS).**
Even if you cannot integrate the IDS with your firewall, run a passive IDS rather than none.

Daily

□ **Port scan server addresses and addresses you assign to DSL and dial-up.** Scanning dial-up addresses enables you to find home users that are infected with Code Red and other viruses. If you detect infection on a user's computer, disable the account and help the user to clean up the computer before allowing reconnection. This tough policy is particularly necessary now that viruses like Nimda and Code Red are out in the wild. Use nmap and strobe.

Weekly

□ **Carry out event and component log reviews.** In RAS logs, watch for large numbers of disconnected users at the same time, which could indicate that something in the RAS pipeline is faulty or misconfigured. For e-mail servers, look for bounced messages, which could indicate that a spammer is using the server. Across all machines, watch for failed logon attempts, which can indicate that crackers are having a go at the system.

□ **Test firewalls from inside and outside using port scanners and any other appropriate tools.** This can include exploits specific to your particular firewall systems. Good security policy dictates that you lock down outgoing services such as port 80 and 21 at the firewall to prevent your servers from being used as attack hosts if they are compromised. It is therefore necessary to test firewalls from the inside to ensure the policy is still in effect.

Tools to use include netcat, nmap, Sniffer Pro, Cyber Cop Scanner, telnet, Internet Explorer, ftp, ping, ping6, tracert, tracert6, wget, strobe, RealSecure, ISS scanner, ARP works (which injects custom arp announcements).

Monthly

□ **Use new security (cracker) tools to find holes in new operating systems or operating systems that are regularly or automatically upgraded.**

□ **Strength test administrative account passwords.** Run a brute force crack program on them such as L0phtCrack.

□ **Test the validity of the access control lists (ACLs) by trying different users who do not have explicit permissions.**

□ **Perform security assessment internet scans.** These scans are more in-depth than a simple port scan. The scans probe communication services, operating systems, applications, and routers to uncover and report system vulnerabilities that could be attacked. Look at what services are running on each particular box, and probe those services for specific exploits.

Policy Security

Constant

□ **Explicitly deny "Logon local permissions to all guest accounts, and non-administrative accounts."**

□ **Explicitly deny "Allow logon through terminal services to all guest accounts, and non-administrative accounts."**

□ **Enable FULL (Success/Failure) auditing in Domain GPO.**

□ **Configure Microsoft Operations Manager (MOM) to send notifications when events like "User added to group domain administrators" happen.** See www.microsoft.com/mom/.

□ **Maintain strict ACLs on all content servers.**
How strict? Aim for no extra permissions. For example, if you have a share on a server, you and the domain administrators should be the only ones who can access it.

□ **Require strong passwords for all users.**

□ **Require extra strong passwords for all administrative accounts.**

□ **Lockout accounts on repeated failed logon attempts.**
Standard practice is to give accounts three attempts, but if you are forcing strong passwords--as Trey Internet does--then you should increase the number of tries allowed. Trey Internet allows 15 attempts and locks out accounts for 30 minutes before re-enabling them.

Monthly

□ **Audit Trey Internet Group Policy Object (GPO).**
Make sure that basic users in Active Directory are explicitly denied access to resources they do not need. Look for rogue accounts that have access to resources they should not.

□ **Audit Active Directory to make sure that user rights are as they should be.**
For example, make sure no dial-up users have gained Terminal Server or administrative rights. This work is a heavy administrative load and should be scripted where possible. For administrative rights, Trey Internet runs:

```
NET GROUP "domain admins" /domain
```

which gives a list of the domain administrators. For Terminal Services, Trey Internet wrote an application which allows them to check and set Terminal Service rights for a user. They load the entire user list, and run this program for all users. Trey Internet limits Terminal Service access to administrators plus only two or three clients whose credentials and needs have been verified.

For dialup, Trey Internet runs:

```
netsh -r dcname ras set user username PERMIT
```

on each user in the user list. They create a batch file for each new user account, and this line is one of the things added to the batch file.

To do this for several accounts at once, save the following to a batch file:

```
REM ------------------------------------------------
rem @echo off

set dcm=treyintdc1
set input_file=input.txt

for /f %%i in (%input_file%) do (netsh -r %dcm% ras set user treyint\%%i PERMIT)
REM ---------------------------------------------------
```

Then create a file called Input.txt with the list of usernames to enable. Run the batch file, and it will pull names out of Input.txt one at a time.

□ **Audit all co-located servers and production servers for services running unnecessarily.**

Firewall and Router Security

Constant

□ **Install ACLs on routers to allow management traffic to and from certain locations.**

□ **Set all ACLs and firewall rules to default deny and logged.**
This means if something is not explicitly listed in firewall rules, it is denied.

□ **Adopt the following firewall rules as a base set:**

- Default deny, explicitly allow services, and explicitly deny others, for additional security.
- Deny all traffic to ports 135-139,445 TCP/UDP (NetBios/SMB).
- Deny all traffic to port 3389 TCP/UDP (Terminal Services).
- Deny all traffic to DCs.
- Deny all traffic to internal DNS servers.
- Allow traffic from firewall management console to firewall.
- Deny all other traffic to and from your firewall.
- Permit only DNS (port 53 TCP/UDP) traffic to external DNS servers.
- Permit only required ports for each service on each server thereafter.

Other

Constant

□ **Run virus scans on all servers.**

□ **Monitor various security distribution lists for hot fixes, and apply them when they arrive.**

□ **During virus outbreaks, block certain mail attachments related or unrelated to the problem, depending on the potential impact.**
Trey Internet uses Trend Micro's ScanMail for Exchange 2000.

Weekly

□ **Monitor number of Non-Delivery Reports (NDRs) generated.**
Given that Trey Internet does not allow its mail servers to relay, a high number of NDRs can indicate that one of Trey's own users is a spammer. To confirm this, check the Exchange server logs and see which specific type of NDR is being generated. If a Trey user has sent the same message to many people, Trey reminds the user of the Terms of Service agreement and tells the user to cease and desist. If the situation occurs again, the user loses the account.

□ **Monitor invalid relay attempts.**
This can indicate a spammer on the Internet trying to relay through Trey Internet's network, though Trey's configuration automatically blocks them by checking for invalid domains or invalid users trying to send mail. Trey looks for excessive client SMTP connections with associated failures in a short space of time. What constitutes "excessive" is a judgment call. Trey also reports the IP address of offenders to their ISP and to anti-spamming organizations.

Monthly

□ **Sweep accounts for users no longer employed at company, partner, or customer companies where possible.**

Physical Security

Constant

□ **Lock all rooms.**
Make sure access is available to a small and known number of people.