10+ reasons to treat network security like home security

Version 1.0
October 24, 2008

By Chad Perrin

Note: This information first appeared in the IT Security blog.

As I pack up my various technical references and novels in preparation for moving, it occurs to me that the front door of your house can teach you some things about IT security.

1 Deadbolts are more secure than the lock built into the handle.

Not only are they sturdier, but they're harder to pick. On the other hand, both of these characteristics are dependent on design differences that make them less convenient to use than the lock built into the handle. If you're in a hurry, you can just turn the lock on the inside handle and swing the door shut -- it'll lock itself and you don't need to use a key, but the security it provides isn't quite as complete. A determined thief can still get in more easily than if you used a deadbolt, and you may find the convenience of skipping the deadbolt evaporates when you lock your keys inside the house.

The lesson: Don't take the easy way out. It's not so easy when things don't go according to plan.

2 Simply closing your door is enough to deter the average passerby, even if he's the sort of morally bankrupt loser that likes thefts of opportunity.

If it looks locked, most people assume it is locked. This in no way deters someone who's serious about getting into the house, though.

The lesson: Never rely on the appearance of security. The best way to achieve that appearance is to make sure you're actually secure.

3 Even a deadbolt-locked door is only as secure as the doorframe.

If you have a solid-core door with strong, tempered steel deadbolts set into a doorframe attached to drywall with facing tacks, one good kick will break the door open without any damage to your high-quality door and deadbolt. The upside is that you'll be able to reuse the door and locks. The downside is that your 70-inch HD television will be fenced by daybreak.

The lesson: The security provided by a single piece of software is only as good as the difficulty of getting around it. Don't assume security crackers will always use the front door the way it was intended.

4 It's worse than the doorframe.

How secure is the window next to the front door?

The lesson: Locking down your firewall won't protect you against Trojans received via e-mail. Try to cover every point of entry or you may as well not cover any of them.

5 **When someone knocks on the front door, you might want to see who's out there before you open it.**

That's why peepholes were invented. Similarly, if you hear the sounds of lockpicks (or even a key, when you know nobody else should have one), you shouldn't just open the door to see who it is. It might be someone with a knife and a desire to loot your home.

The lesson: Be careful about what kind of outgoing traffic you allow -- and how your security policies deal with it. For instance, most stateful firewalls allow incoming traffic on all connections that were established from inside, so it behooves you to make sure you account for all allowable outgoing traffic.

6 **Putting a sign in your window that advertises an armed response alarm system, or even an NRA membership sticker, can deter criminals who would otherwise be tempted to break in.**

Remember that the majority of burglars in the United States admit to being more afraid of armed homeowners than the police, even after they've been apprehended. Telling people about strong security helps reduce the likelihood of being a victim.

The lesson: Secrecy about security doesn't make anyone a smaller target.

7 **A good response to a bad situation requires knowing about the bad situation.**

If someone breaks into your house, bent on doing you and your possessions harm, you cannot respond effectively without knowing there's an intruder. Make sure you -- or someone empowered to act on your behalf, such as an armed security response service, the police, or someone else you trust -- have some way of knowing when someone has broken in.

The lesson: Intrusion detection and logging are more useful than you may realize. You might notice someone has compromised your network and planted botnet Trojans before they're put to use, or you might log information that can help you track down the intruder or recover from the security failure (and prevent a similar one in the future).

8 **Nobody thinks of everything.**

Maybe someone will get past your front (or back) door, despite your best efforts. Someone you trust enough to let inside may even turn out to be less honest than you thought. Layered security, right down to careful protection of your valuables and family, even from inside your house, is important in case someone gets past the outer walls of your home. Extra protection, such as locks on interior doors and a safe for valuables, can make the difference between discomfort and disaster.

The lesson: Protect the inside of your network from itself, as well as from the rest of the world. Encrypted connections, such as SSH tunnels even between computers on the same network, might save your bacon some day.

9 **The best doors, locks, window bars, safes, and security systems cannot stop all of the most skilled and determined burglars from getting inside all of the time.**

Once in a while, someone can get lucky against even the best home security. Make sure you insure your valuables and otherwise prepare for the worst.

The lesson: Have a good disaster recovery plan in place -- one that doesn't rely on the same security model as the systems that need to be recovered in the event of a disaster. Just as a safety deposit box can be used to protect certain rarely used valuables, offsite backups can save your data, your job, and/or your business.

10 **Your house isn't the only place you need to be protected.**

A cell phone when your car breaks down, a keen awareness of your surroundings, and maybe some form of personal protection can all be the difference between life and death when you're away from home. Even something as simple as accidentally leaving your wallet behind in a restaurant can lead to disaster if someone uses your identity to commit other crimes that may be traced back to you, to run up your credit cards, and to loot your bank accounts. Your personal security shouldn't stop when you leave your house.

The lesson: Technology that leaves the site, information you may take with you, such as passwords, and data you need to share with the outside world need to be protected every bit as much as the network itself.

I promised 10+ in the title of this article. This bonus piece of the analogy turns it around and gives you a different perspective on how to think about IT security.

11 **Good analogies go both ways.**

Any basic security principles that apply to securing your network can also apply to securing your house or even the building that houses the physical infrastructure of your network.

The lesson: Don't neglect physical security. The best firewall in the world won't stop someone from walking in the front door empty-handed, then walking out with thousands of dollars in hardware containing millions of dollars' worth of data. That's a job for the deadbolt.

Okay, back to packing. I've procrastinated enough.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our IT Leadership Newsletter
- Check out all of TechRepublic's free newsletters
- 10 common security mistakes that should never be made
- 10 things you should do to secure every general-purpose operating system
- 10 things you should do to ensure basic Web site security

Version history

Version: 1.0
Published: October 24, 2008

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 Content Team