ALEXANDER MUENTZ

script kiddies with briefcases

THE LEGAL SYSTEM AS THREAT

Alexander Muentz is both a sysadmin (since 1999) and a lawyer (admitted to the bar in Pennsylvania and New Jersey). He'd love to be a hacker public defender but has to earn his living helping law firms do electronic discovery. When he's not lawgeeking, he tries to spend time with his wife and his motorcycle.

lex@successfulseasons.com

Sysadmins have to know more than just their systems to do their jobs well. You have to understand people, finance, and your organization's business to spend its money wisely and protect it from all sorts of threats. IT people tend to think of threats using an preparation/attack/response framework, even when the threats are not malicious. You can then compare risks and allocate resources rationally. If threats can affect your systems, your users, or their data, they should be on your mind, even if most of the responsibility rests on someone else.

So why not think about legal processes in the same way? Some resemble existing attacks (having your systems seized is like a DOS attack), whereas others are unique. I'll discuss search warrants, wiretaps, subpoenas, and discovery orders and their effects on users, systems, and data. Because this is a significantly deeper subject than can be explained in a small book, let alone a single article, I'll just be glossing over important nuances to give you an overview of the issues. This article only discusses U.S. federal law, but many state laws resemble federal ones. This isn't legal advice so much as it is the start of a conversation that you can finish with your IT staff or legal counsel. Let's talk about a few threats.

The Search Warrant: Noisy, Disruptive, and Potentially Destructive

A search warrant execution to an IT defender is like an invasion and a DOS attack wrapped up together. Law enforcement officers (LEOs) enter the area with enough strength to control the area and to prevent evidence or people of interest from leaving. Intimidation is a second benefit to such overwhelming force—scared people often unknowingly waive their rights.

A search warrant is a legal document issued by a neutral judicial officer such as a judge and specifies both the area to be searched and what is to be searched for and taken or seized [1]. There are some specifics about how the warrant is obtained, but I'll not delve into that for two reasons: (1) they're rather complex (even to lawyers); (2) you can't stop or interfere with a search while it's being executed. Your concern should be limited to two

potentially conflicting interests: preventing disruption to your organization, and not waiving your rights.

It helps to focus on the three distinct phases of such a legal attack:

- Pre-attack: Defenses include redundant systems in multiple places, good backups, and an attorney on retainer who is familiar with your operations.
- During the attack: Either be quiet or helpful. Protect your rights. Don't interfere.
- Post-attack cleanup: Transfer over to untouched systems and restore from backups. Attack the warrant and file suit for damages and/or return of equipment or data.

During the Search

LEOs with a warrant to search and seize electronic evidence have some discretion about the execution. They can take copies of the evidence, media, or entire systems that they believe contain what they're looking for [2]. Although letting them take forensic copies of your systems may be annoying, wholesale removal of several servers is far worse. There's an obvious temptation to assist the LEOs so that they don't feel the need to truck your entire server room back to their office. Generally, I'd recommend keeping the conversation to a minimum, both to stay safe and to prevent expansion of the scope of the search. LEOs can expand the search if you grant permission, which you may do during the course of the discussion. You may also unintentionally admit knowledge of or control over evidence, which may make you "of interest" to the LEOs. That's not a good thing. Ever.

Imagine the following hypothetical situation: An LEO arrives with a warrant to search system A1 for Alice's email. Bob is the sysadmin for A1 and A2. The LEO, while debating on whether or not to put A1 on a hand truck, asks Bob if he can look at Alice's files on A2 or Abe's files on A1. If Bob doesn't clearly say no, the LEO may start looking. Or, imagine that the LEO's warrant includes A3, a system on which only Alice has a login. If Bob, attempting to be helpful, knows Alice's password on A3 and gives it to the LEO, he's now opened himself up to possessing whatever is on A3.

I want to end this section with two final ideas of what to do during the search. First off, *do not interfere with the search*. Such behavior may subject you to several criminal charges, in addition to charges related to whatever the search was about. Second, have a witness or two available to watch. You may want an additional person who can say what happened during the search, in case your recollection disagrees with the LEO's.

After the Search

If you have good backups or alternate sites, you can recover or cut over, minimizing your total outage. If the LEO took any systems, your lawyer can sue for their return [3] and also attempt to exclude the evidence from trial if there's a flaw in the search warrant (evidence gained from a incorrectly obtained or executed warrant can be suppressed prior to its admission in court).

Wiretaps

IF YOU'RE THE TARGET

The attack profile: Quiet and incriminating.

- Pre-attack: Defenses include point–to–point encryption under your control.
- During the attack: There's no defense. If the wiretapping is done correctly, you won't know until it's too late.
- Post-attack cleanup: Suppress the evidence in court.

Wiretaps aren't just for phones any more. LEOs may intercept IP traffic with a valid wiretap warrant or with the permission of the intended recipient [4]. I'm not going to discuss Foreign Intelligence Surveillance Act (FISA [5] wiretaps because I think that's still a moving target. I hope it will be rare for readers to be the target of a regular LEO wiretap (also known as a Title III [6]), but I think it's helpful to understand them.

An LEO with a warrant can request that a wiretap be placed somewhere on a network where it can acquire all the traffic sent and received from the target, without the target's knowledge. It is unlawful for the wiretap to acquire "innocent" traffic, and this responsibility falls to the provider of the network, not the LEO. Encryption can shield the communications as long as it takes to decrypt the traffic or acquire the key. If the service provider has the key, the service provider can be forced to divulge it with a court order. Although the key may be acquired with a search warrant or subpoena, at least the target is informed of the lack of privacy.

IF YOU'RE THE PROVIDER OF THE SERVICE

The attack profile: Confusion, stress, and expense.

- Pre-attack: Defenses include the ability to carve out traffic to any host or user.
- During the attack: Have network staff ready to assist the LEO.

Providers of electronic communication services must accommodate valid wiretap warrants, allowing LEOs to remotely acquire targeted traffic while ignoring innocent traffic [7]. The provider must carve out any requested IP traffic or communications and forward them to law enforcement. If the provider encrypts the traffic, it must also decrypt it or make the keys available as well. There's some controversy about who is a "provider" under this legislation, as well as whether or not the wiretap can be remotely activated without the intervention or knowledge of the provider. But such controversy is the subject of another article.

SUBPOENAS AND DISCOVERY

The attack profile: Slow but invasive.

- Pre-attack: Defenses include a data retention/destruction policy. You need to be able to search all of your storage for relevant documents.
- During the attack: Work closely with legal representation.
- Post-attack cleanup: Expect repeat requests and be ready to explain what you did.

Although there are some legal differences between subpoenas and discovery, the two are similar from an IT defender's point of view. They're both legal orders to provide information, and since more information is stored electronically, you're going to be asked to help out if your organization is served with a subpoena or is a party to a lawsuit. Being able to retrieve information quickly and to honestly claim that you've searched all your files will make you golden.

First off, a sensible data retention policy is important. Talk to your counsel about what you have to keep and for how long. Be willing to explain how backups work in layman's terms. Once you have a retention policy that you can live with, follow it. If it says keep data for no longer than three years, make sure you've erased or destroyed older media. This dovetails into the second half of your pre-attack defenses. Knowing what you have prevents expensive mistakes.

A short war story is worth recounting here: When I was a backup admin, I was helping an outside law firm in searching through our archives. After searching the backups that I knew about, I gave them all the documents matching the search terms the form provided. Imagine my surprise when someone found a crate of DLTs from before my time, but within the scope of the request. The outside counsel almost had a heart attack. Lucky for us, the tapes had been stored above a Nuclear Magnetic Resonance machine, and they were all blank. Discovering relevant information later makes you look dishonest, and hiding it would have made us dishonest.

SUBPOENAS AND DISCOVERY: WHERE THEY DIFFER

Subpoenas do the heavy lifting in legal investigations. Grand juries, regulatory agencies, and courts can all issue them. The two basic types of subpoenas are *Duces Tecum* (bring us stuff) and *Ad Testificandum* (come and testify under oath). You can also get one if your organization has information necessary to resolve a lawsuit between other people. Dealing with a subpoena is less disruptive than a search warrant—you usually have a few days to respond at the minimum. If the request is difficult to comply with, counsel may be able to narrow the scope to make it easier. (Don't you wish you could do that with your other projects?) Unfortunately, not too much is protected from a subpoena other than trade secrets and some client-attorney communications (for example, Rule 45 of the Federal Rules of Civil Procedure protects trade secrets and communications normally under some privilege). As long as it isn't abusive, overly burdensome, or not likely to lead to relevant evidence, it may have to be brought to the issuer.

Discovery entails sharing of relevant information between parties. Simply put, if you are in a lawsuit, you have to give the other side any information (discovery) you have that may help your adversary's case. You also have a duty to preserve any of that information when litigation becomes likely. So does your adversary. The only relevant information that you can withhold are some attorney-related files. Under the new Federal Rules of Civil Procedure, litigants must either hand over discovery that is in electronic storage or divulge the nature and location of that discovery fairly soon after the lawsuit is filed [8].

WORKING CLOSELY WITH YOUR LEGAL COUNSEL

When your organization has been served with a subpoena or discovery request, someone has to collect all the information that "responds" to the request. You'll be collecting a lot of it, and counsel will be reviewing it to see whether it's responsive. Your lawyers will be pulling long hours looking through each file you bring them. They'll need help with viewing, sorting, and interpreting the mountain of data. This may require them to hire temp workers or to export the files to their outside law firm. Being helpful here will let your organization save money and effort.

You may be called on to explain what you did in collecting the information, either to opposing counsel or at a grand jury or trial. If this is a discovery request, there are a few additional ways you can help. First, you can identify information that you hold that is very time-consuming or expensive to deliver, such as data on obsolete or failing media [9]. Counsel can go back to the court and exclude or reduce the amount of such discovery.

Conclusion

In closing, knowing what I just told you might allow you to be proactive when dealing with your organization's legal department, instead of waiting for the lawyers to come and impose difficult rules upon you. Let them know that you want to coordinate defenses and protect your users and the organization as a whole. They may be pleasantly surprised.

REFERENCES

[1] U.S. Constitution, Amendment 4.

[2] "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," CCIPS, Department of Justice (available at www.cybercrime.gov/s&smanual2002.htm).

[3] Federal Rules of Criminal Procedure, 41(e).

[4] 18 U.S.C. §§ 2518, 2511(2)(c).

[5] FISA (50 U.S.C § 1801 et seq).

[6] Title III of the 1968 Omnibus Crime Control Act. It's been modified by subsequent legislation, including the Stored Communications Act (18 U.S.C. §§2701-2722), Electronic Communications Privacy Act (18 U.S.C. §§ 2501 et seq) and a few others you may have heard of.

[7] CALEA, 108 Stat 4729.

[8] See FRCP 26(a)(1)(B).

[9] See FRCP 26(b)(2)(B).