Corporate Security

Description: Steve and Leo discuss the week's major security events, then use a listener's story of his organization's security challenges to set the stage for their discussion of the types of challenges corporations face in attempting to provide a secure computing environment.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-127.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-127-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 127 for January 17, 2008: Securing the Enterprise. Security Now! is brought to you by listeners like you. Thanks for your support.

Time for Security Now!. I'm Leo Laporte, feeling a little bit better. Steve Gibson is, as always, the peak of health because he never leaves his Irvine security lab.

Steve Gibson: That's right, my antivirus, disinfected tower of health.

Leo: I tell you, I'm going to start wearing surgical masks on planes, I think. I really - this is the worst. Although, you know, I don't know if it's consolation, but I've talked to so many people who've had terrible colds this year. Whatever that cold is that's going around is a doozy. Don't get it.

Steve: I'm going to work on that.

Leo: That would be my advice to you. Stay away from it. So we had a fun time last week answering a lot of questions. What are we going to do this week to top that?

Steve: Well, actually one listener wrote a long sort of, well, explanation about his company's problems with enforcing security policy. And I really liked it. And it sort of brought up the whole issue to me that we haven't ever really discussed before of the challenges of corporate IT security policy and enforcement, the inherent tension between the security staff, you know, IT and employees. So I just sort of wanted to talk about some of the things that I think that both

employees face and corporations face in this battle to secure a typically very heterogeneous, complex, and more complex every day environment.

Leo: Yeah. It is, it's a real - I do not envy our IT pro friends because they've got a real task. Even worse, I mean, imagine how hard it is - it's bad enough you have to lock your own system down - locking down the systems of hundreds of thousands of users, all of whom have their own ideas about what they want to do on that computer.

Steve: Exactly.

Leo: But before we do that, is there any news in the security...

Steve: Oh, there was a bunch of stuff this week that was really sort of interesting and fun. Last week we talked about, you may remember, Master Boot Record, that is to say, MBR rootkits. Okay? Last week they were theory. This week they are in the wild.

Leo: Wow, that was fast.

Steve: It turns out that there are four vulnerabilities which are known and have been patched. Microsoft has a JVM, a Java Virtual Machine byte-verify vulnerability; a problem with MDAP, which is one of their database APIs; a different problem with Internet Explorer's Vector Markup Language, the VML vulnerability; and a problem with XML core services. Those four different problems are being used to install, currently install, a new set of Master Boot Record rootkits. These have been found in the wild. So when someone visits a hostile web page - and we talked about before, this is sort of pretty much the typical way bad stuff now gets in your machine is that one way or another you are tricked into going somewhere bad. And a known vulnerability, hopefully a known vulnerability, which hopefully you've patched, will try to do something bad to you.

Again, if you're current, and if Microsoft knows about this - or I don't mean to just blame Microsoft. I mean, there are in fact, for example, there's now proof-of-concept code out for a new QuickTime remote code execution vulnerability that affects both Mac and Windows. Now, of course, it would have to be different code in order to run in a Mac than would run in Windows. So the same exploit of that vulnerability could not be used across both platforms. But both of them are vulnerable because they both are using QuickTime. And this was something that came out with zero day, so Apple wasn't even aware that this existed when this thing first showed up. So this is typically what's happening.

The really scary thing is, being a rootkit, this thing gets control of and patches the OS before it loads. That is, in this case it is a Windows-only MBR rootkit. And it makes itself undetectable by antivirus software. So it's a rootkit in the pure sense of getting in and modifying the kernel prior to loading in order to protect itself.

Leo: Now, the anti-rootkit programs like RootkitRevealer from Mark Russinovich, BlackLight from Frisk, those would work against something like this; right?

Steve: I don't know at this point. This is so new that not much research has been done. I haven't seen this myself, and I haven't read much about it except that these things are now in the wild. And what's sort of interesting, too, is that this is what we faced 15 years ago with the very first viruses. I mean, when people were using so-called "sneakernet" to - by mistake you'd

get floppies that would be infected, and you'd stick a floppy in someone's computer. And when you accessed it, it would install itself over on that machine's hard drive. I mean, this is - we've seen in the old days Master Boot Record viruses that sort of were all in fashion for a while, then went away. And as security has tightened up everywhere else, this is one little hole that has never been patched in our newer machines. And so it's been sort of rediscovered as, hey, look, we can still infect the MBR, and that'll give us control before the OS boots. And using state-of-the-art techniques now to analyze code, it's much easier to patch someone on the fly and modify the kernel as it comes up.

Leo: Right. A traditional rootkit would get run at some point during boot-up, just not so early.

Steve: Exactly. Normally, if, for example, it installs itself as a device driver, a boot-time device driver, which the OS would unwittingly load, and then being in the kernel as device drivers are, gives that thing a lot of control. They would then go about patching the kernel in order to obscure its own presence.

Leo: So by loading in the Master Boot Record, what is the advantage?

Steve: Well, the advantage is that literally nothing is running. That is, the way...

Leo: No security software, nothing.

Steve: Well, literally yes, nothing.

Leo: Not even Windows.

Steve: That first sector is loaded into raw memory. And in fact the system is not even in protected mode. It's in real mode, which is the way this code runs. So there aren't even protection services available from the chipset at that point. I mean, it is literally - the BIOS has run at that point. But then the system's in real mode. That one sector, that 512 bytes, is copied into a location in low memory. Then that sector is jumped into, that is, that chunk of memory is jumped into and executed. That normally then goes about finding the beginning sectors of the bootable partition, which it then loads into memory and then runs. In this case, it loads more of itself, that is, more of the first track of the hard drive where this thing lives in order to get conscious enough to do the kind of damage that it needs to. It then goes out and patches, on the fly patches the operating system, which then boots, although it's already been infected.

So it's spooky stuff. No doubt the AV people will get on this. Microsoft will get on this because you are running in Windows when you are caught by one of these Microsoft vulnerabilities, which then allows the Windows executing code to install that Master Boot Record code on the hard drive. So that's the hole that next needs to get plugged.

Leo: Right, right. That's when security software's running, and you can watch for that kind of thing.

Steve: Right. Also last week we talked about how 70,000-plus sites had been infected by malware recently. That is, it was JavaScript that was being installed, taking advantage of some

SQL vulnerabilities in order to compromise websites with exactly this kind of malicious software. What's just turned up recently is a new twist on this. The way they knew it was 70,000 is that this malicious JavaScript was appearing on web pages of sites that were being dynamically generated. You know, basically there was an SQL database on the backend that was serving pages dynamically. That got infected, that is, the SQL tables got infected, which caused it to put this malicious JavaScript on these pages. Well, the way people knew, for example, it was 70,000 was that they simply Googled some of the malicious JavaScript, and Google had already been out there browsing around, dutifully cataloging all these pages, so it was easy to find. The newest twist, which has just appeared, is there is now polymorphic JavaScript that has been created which renames itself and reorganizes itself and is not broadly searchable in the way that static JavaScript can be.

Leo: It's different on every page.

Steve: Exactly. So naturally, I mean, what we're seeing here in the standard sort of cat-and-mouse game between malware and antimalware forces, is that the bad guys have said, okay, we don't want you to know that it's 70,000 sites. In fact, we don't want you to be able to find us at all. So what they've done is they've just upped the ante again by making their own malicious script modify itself so that you can't use a search in order to quickly find it all, notify those websites, and get this stuff removed. So this is a serious increase in escalation of this problem. Also in this week's news - you're going to get a kick out of this one, Leo. The gray hat hackers have been zeroing in on taking advantage of UPnP-enabled routers.

Leo: Ah ha. You've been warning against UPnP for some time now.

Steve: From, yes, from the first moment this bad idea appeared I've been saying, and I know that you've been repeating, for example, in your various other venues, the danger, the inherent danger of leaving UPnP enabled on routers. There are now some hacker sites that have succeeded in using, first, cross-site scripting; and, more recently, known vulnerabilities in Flash v8 or later. In other words, they're able to take Flash content, and Flash v8 has become so powerful, there is a navigate-to-URL function and a URL request object that can be used to generate local LAN traffic. That's all you need in order to talk to a router that has Universal Plug and Play enabled and use the UPnP technology to rewrite the DNS server or open holes through the router to allow ports to be exposed to the outside. All of that's been done. So we don't yet have any malicious - we don't know yet that there is any malicious code which is doing this.

But this is what, you know, I've been predicting would happen from the beginning because it's just - it's too powerful, and there's no security model associated with this first version of Universal Plug and Play that all routers, now all consumer routers have, and which most have, unfortunately, enabled by default. So again, this is different than the Windows defect which was discovered a long time ago and for which I created the Unplug n' Pray freeware. What that did was, there was a remote code execution vulnerability in the original Windows XP Universal Plug and Play service that was running on Windows by default. I was arguing that - and of course we had no XP firewall on by default. And it wasn't until Service Pack 2 of XP that the Windows XP firewall was running. So I argued that there was no reason to have that server running. And so my little Unplug n' Pray utility just disables, it stops and disables the SSDP service, which is the Simple Service Discovery Protocol, in Windows XP.

Well, that's different from routers, that is, the NAT routers that everyone is using now, hopefully everyone, to protect their borders and to allow them to share a single IP, a single public IP among multiple machines in their own LAN. Most of the routers have this Universal Plug and Play technology, the idea being that it solves the problem of NAT traversal simply by opening ports through the router to allow, hopefully, expected and solicited traffic to come back in through the router. The problem is, there's no security model for that. That is to say, any

packets that are generated on the LAN inside can discover the presence of Universal Plug and Play services and talk to them and cause them to do things.

So I would once again say to all of our listeners to take this seriously. What this means is that at some point in the future, as we've been predicting, there will be malware which, once it gets on your machine, reconfigures your router behind your back to do things you don't want to do, or don't want it to do. For example, changing your DNS to something fraudulent means that all of the machines you've got will be going to some bogus DNS server to pick up the IPs of common URLs, which is, I mean, that's everything that phishing sites want. I mean, it's like the holy grail of redirecting your computers to malicious spoofing sites. So we're getting closer to it.

Leo: So the best thing to do is go into your router and disable UPnP.

Steve: Yes, yes.

Leo: I mean, you've been saying that for some time.

Steve: Exactly. Now, there are going to be some side effects to it.

Leo: You know what I hear from people a lot is Xbox Live. Unfortunately, Xbox Live has this little feature where you can check - I forgot what they call it. But it's definitely a euphemism. But you could check your accessibility to other players.

Steve: Right. And I think there are, like, three grades of accessibility. It turns out...

Leo: They encourage you, basically, to turn on UPnP.

Steve: Unfortunately they do. It turns out, though, that there is a very simple set of static ports which you could map through. You could disable Universal Plug and Play, reboot your router so that you flush any existing mappings that may have already been set up. Then you can do your own static port forwarding of just a couple ports. And it's not many. It might even only be one. But I remember that it's at the most just a few. Map them through to the IP of your Xbox, and then you're okay. Then it's happy, it's completely on the 'Net, it's fully game enabled; yet you haven't had to turn Universal Plug and Play on in your router in order to get there.

Leo: It's unfortunate because most people who want to play Xbox aren't necessarily that sophisticated.

Steve: Exactly.

Leo: It is two ports. It's UDP 88 and 3074 on UDP and TCP. I'll put a link in our show notes for the settings and Microsoft's tech note on how to do that, for people who want to do that. Maybe help your friends. Because unfortunately what's happening is a lot of kids are basically disabling their router's security so they could play Xbox Live games with their friends. It's kind of the problem.

Steve: Okay. Alex Eckelberry, our friend at Sunbelt Software, reported in his blog and has some nice screenshots of, get this, a new trojan. It's called the Delf.ctk trojan. When you get your computer infected with this thing, it puts up a screen that looks convincingly like Microsoft's Security Center, informing you that - it says, quote: "Error. Browser's security and anti-adware software component license exprited." Got their little typo there. It meant to say "expired," but it got a couple letters wrong, "exprited." It says...

Leo: That's what you always look for, by the way, is grammatical and spelling errors.

Steve: Exactly. Well, yes. Then it says: "Surfing porn, adult and some other kind of sites you like without this software is dangerous and threatens with infection of your computer by harmful viruses, adware, spyware, et cetera."

Leo: And its recommendation would be...

Steve: Oh, first of all, it takes over your machine, locks it up. There's nothing you can do. It requires that you make a call to a 900 number.

Leo: Oh, dear.

Steve: Which costs $35. So basically this is a $35 phone call extortion trojan.

Leo: Oh, my goodness.

Steve: And one of the - there are several numbers it gives. One of them, for example, is a number that ends up going to the West African nation of Cameroon, where there is a call center. You have to enter a PIN, I mean, the screens are, you know, obviously not grammatically very convincing. But the user has no choice. I mean, literally you have to call...

Leo: There must be something you can do. You don't have to call that number, do you?

Steve: Well, Alex says that your machine is locked up. And the only way to get this thing to leave you alone is to call the number, you enter some PINs that come up on the screen in order to - which costs $35 - in order to get your computer back.

Leo: That's appalling. That is just appalling. Now, you would get - this is a trojan. So you get it in your email and you run it, or you get it by going to a website that's been compromised, and you haven't done your updates, things like that.

Steve: Yup. It gets onto your machine, and then it says, okay, we're going to charge you $35 to have your computer back.

Leo: Now, if you have an antivirus running, and you accidentally open this file, will it still infect you?

Steve: I don't know whether AV is yet up to speed. This apparently is pretty new. So certainly, again, standard practice is keep your AV patterns up to date.

Leo: Sure. But even then, don't open attachments.

Steve: Yup. There was another little blurb that I wanted to mention. I was just setting up a brand new little HP machine. I got a couple little HP Pavilions just because they were sort of small and cute, and they're nice for various single purposes. I was shocked by the amount of what now the industry is beginning to call "crapware" that was preinstalled on this thing. I mean, it was unbelievable. Well, the point is that it turns out that there is now the third in a series of zero-day remote code execution flaws in the preinstalled HP software. So...

Leo: Oh, my god.

Steve: Yeah. So not only is this stuff annoying, all this demoware and junk that you didn't ask for, but the problem is that it's got security flaws also which are generally much less maintained than the stuff from Microsoft. So I did have an experience also with both a Dell laptop and a Dell desktop recently. And I was holding my breath when I booted them the first time, thinking, oh, god, you know, how much junk is there going to be on it? And the answer was, like, none.

Leo: Well, Dell has this new thing where you can order it without the crapware.

Steve: And, yes, on their site they're even boasting that there is no demoware installed on these machines. And I thought, well, that's, I mean, it has been my experience with two recent Dell machines that they're no longer loaded with all this junk that you don't want.

Leo: They're listening to their customers. Do you know what the HP demo is that has this exploit in it?

Steve: It is HP's Remote System Update.

Leo: Oh, good. Now, presumably HP will patch this.

Steve: They have before. Three times this has happened. And there's now another instance of it.

Leo: Good lord.

Steve: So, yes, and so it's not just a matter of this stuff being unwanted. It's also insecure.

Leo: Dangerous, yeah.

Steve: Okay. And finally, this is just too bizarre, but I had to share this with our listeners.

Digital picture frames are now infecting PCs with malware.

Leo: You're just full of good news today.

Steve: There have been multiple reports of people using a USB key to transfer photos to digital picture frames, which in turn, the firmware on the frames installs PC malware onto their USB drives, which then, when plugged back into the PC, take over the PC.

Leo: Wow.

Steve: And these are brand new, from the factory, digital picture frames.

Leo: Which manufacturer?

Steve: I don't have any names.

Leo: Geez. All right.

Steve: But because there have been multiple reports of picture frames doing this. In some cases, some of them were resold. But it has been also confirmed in brand new digital picture frames that there is malware installed on them that then jumps to the USB storage and then over to a PC.

Leo: Wow. This is from Security Focus, this story. So I'll put a link in the show notes to this, as well.

Steve: Yeah, and I think Computer World also reported that, as well. So it's just like, oh, my god. I mean, this is the law and the rule that we learn about security is, if it can be done, it will be done. This is what led me to believe Universal Plug and Play from the first moment I saw it was a bad idea. And similarly, the MBR rootkit is another example of that. It's just...

Leo: We're going to see more of this, too, because, you know, these digital picture frames are a perfect example. We are now surrounding ourselves in our lives with little computers executing code.

Steve: Right.

Leo: And they talk to everything. You know, that's scary.

Steve: Yup. Well, I did want to share a short and sort of fun SpinRite anecdote with our listeners. This is from a guy named Charles Hayes, who wrote to us, oh, on the 12th, so just five days ago. He says, "I purchased SpinRite around May or June of 2006..." So that was about a year and a half ago. He says, "...and it saved me from reinstalling Windows. My computer

would reboot every time I clicked on one particular email. Also when I tried to compress the folders in email it would reboot. And I could not run Windows Defrag. I remembered about SpinRite on the Screensavers..." You know, your old show on Tech TV, Leo. And he said, "...and I purchased it. I ran it, and it fixed the problem completely." So that's a year and a half ago.

And he says, "A few days ago my computer would reboot on its own, usually within 30 minutes to an hour after I logged in. I tried different memory, and that didn't help. I thought I might have to buy another motherboard. But I ran SpinRite again, and it found one area with unrecoverable data and repaired it." He says, "I figured that may be the problem. And sure enough, when I rebooted back into Windows, it's been running perfectly ever since." He says, "This product has been a lifesaver for me more than once. I'll just have to start running it more often. Thanks."

And that really is the lesson that I wanted to convey in this little note is, you know, Charles had it, it fixed his problem a year and a half ago. And another problem obviously occurred on that same drive. And at that point it was really causing him trouble. Clearly, had he run SpinRite every six months, I mean, I recognize it takes a long time to run because it's doing a lot of work on drives which have become massive. So it's not something convenient to do weekly. But every six months, for example, would have prevented this problem from occurring, and it would have probably been able to recover whatever data was in that sector. And I'm not sure that it wasn't able to, or perhaps did a partial recovery. But again, you really don't want to let too much time go by. So if nothing else, I would remind current SpinRite owners that they can get some benefit from running it even when it hasn't - when it's no longer a matter of life and death.

Leo: Prophylactically, as we say.

Steve: Yes, exactly.

Leo: All right, let's hear this letter from your IT professional.

Steve: Yes, this is Dennis in Halifax, Nova Scotia. He said, "Hi, Steve. I work on a help desk in a government department in Nova Scotia, Canada. Including our department and other agencies, we support about a thousand users." So he's on a help desk in a government agency with a thousand users that he supports with his help desk. He says, "The problem I have is that no one here seems to take electronic records, computer security, or data integrity at all seriously. The data we deal with is extremely sensitive and includes a lot of personal data - medical records, health information, and much more. Not only do we have problems with computer-related security, but also with physical security. The building I work in is really a joke. We have a security person down on one of the main floors, and the doors all have key cards. But during normal business hours all it takes is a walk around the back of the building to get to the floor below, then a short ride in the elevator to get you to any floor in the building. Once on any given floor, there's a keypad on each door. But the code has only been changed once in the past few years."

Leo: So everybody who ever worked there knows it.

Steve: And he said, "Every employee and former employee knows the code to almost every door because it's the same for each floor. Oh, and almost every employee will let just about anyone standing by the door in without any question, whether they recognize them or not."

Leo: What do they call that, tailgating?

Steve: Exactly, tailgating. And in fact it's funny because when I was setting up my access to Level 3 I was specifically told, you scan your card, you stick hand in the biometric hand scanner, and the door unlocks. And they said, we're sorry, but do not let somebody else who approaches you in. Apologize to them and say, I'm sure you understand, I can't let you in. Close the door and then make them go through the same process. So, yeah, but again, it's hard to enforce that social policy.

Leo: It is. And Canadians are friendly. That's your problem right there. They're nice guys.

Steve: Exactly. He says, "Recently a new policy came down from our CIO's office stating some key security points. The main ones were: Laptops must have encryption; Blackberries must be password protected; we're not allowed to use any means, parens, (electronic or otherwise), to remember passwords; we must also..."

Leo: Really. They can't use, like, RoboForm or some other...

Steve: Apparently no electronic or otherwise means to remember passwords. You just have to memorize them. Of course we know the problem with that is then people will choose easily guessable passwords. He says, "We also have a draft, but considered the working copy, Acceptable Use Policy - AUP - that prohibits the use of peer-to-peer software such as LimeWire, BitTorrent, et cetera..."

Leo: Or Skype, as we were talking about last week.

Steve: Exactly. "This policy also prohibits the use of any instant messaging software such as MSN, ICQ, AIM, et cetera, because they are supposedly not secure." He says, "The problem with this new policy and AUP is that no one is willing to enforce it. I brought it up at a staff meeting with our team, including the manager, and was basically shot down and told that we can't do what the policy says we need to do. Does this seem wrong? I mean, the policy is not something that I would consider to be at our discretion to enforce. I assume, maybe incorrectly, that a policy is above us all, especially when signed off by the highest ranking person in our organization.

"I suggested in this staff meeting that we really should look at whole-disk encryption because more and more users have been purchasing notebooks and are traveling all over the world with them. I was told there was not enough information in this policy for us to know what we need to do. I agree with that because it didn't mention any level of encryption or which methods should be used. But it really wouldn't be hard to find out by asking the right questions. I'm guessing that that part might be left enough at our discretion since the people who created the policies are not overly technical.

"The last sore point I have is that our organization doesn't even have a data classification scheme. We have no way of telling how confidential or public our documents, files, and records are. I believe this would be the first step we need to take in order to help provide the groundwork needed to base the rest of our security process and procedures on. The whole thing is very frustrating because I believe I have a decent grasp of security concepts. But since I am just a low-level help desk staffer, the higher-ups don't pay any attention to what I have to say. Do you have any advice on how to help convince my organization that security is important?

P.S.: My apologies for writing such a long message. Thanks, Dennis."

Leo: Well, but he raised so many interesting questions.

Steve: Yes. I just - I really - I liked his note because, I mean, you can imagine how many people are sitting around feeling a similar level of frustration. And, I mean, we sort of - we've talked around these things in many of our podcasts. We've never really talked about the challenge that corporate IT faces when it comes to enforcing security policies.

Leo: Well, it's especially difficult when you're a government agency because you also have - and this is not just true of government agencies, but healthcare agencies. A lot of companies have a higher responsibility for security even than just a normal enterprise.

Steve: I have a really good buddy who spends a lot of time working with corporate - working in corporate environments, generally small companies, trying to help them with their security and interacting with the employees. And one of the things that I think is a fundamental sort of like root cause of a lot of the problems is that the computers that people use in their corporate environment are almost universally exactly like the machines they use at home.

Leo: Right. Why can't I do the same things I do at home?

Steve: Exactly. Or they've got - they're like, well, wait a minute, my eight year old is able to use this machine and doesn't seem to have any problems. Why can't I do on my work machine the same things I do at home?

Leo: I think it's a communications issue, too. I think, if you're going to insist on an onerous, what's a seemingly onerous policy, you've got to be very clear and spend a lot of time with your employees explaining why it's necessary and what the risks are. I think a lot of it is people just underestimate the need for security.

Steve: Well, yes, and we hear enough now that people are receiving email, clicking on a link, and getting malware installed on their machines just by doing that. So of course then corporations say, okay, we're not going to allow attachments. And so then people are upset because it's like, okay, wait a minute, but what about good attachments? And the IT policy is, well, there's no way to really be sure that it's a good attachment, so we're just going to say no attachments.

Leo: Right. It's very difficult. And I don't envy the guys who have to do it. And I also am sympathetic with employees because imagine being the IT guy at Tech TV, where you have all of these tech-savvy people who are not easily going to go along with anything you say and who are going to try to get around anything you do.

Steve: And that's a very good point, Leo. It's one that I had on my little outline for things I wanted to remember to mention. And that is exactly that, because computers are so ubiquitous now, to some degree even the common users feel like I know what I'm doing. I have one at home. My eight year old has one. I've got a laptop. Who are you to tell me what I can and cannot do? Because, I mean, everyone to some degree feels like they're something of an expert.

It used to be, remember in the mainframe days you literally had the computer on an elevated floor in an air-conditioned area. And, you know, technicians walked around in white lab coats. And there was this sense of, oh, you know, I don't know what all that is. But, whoa, that seems very impressive. Well, nothing is impressive now seeming about a work machine. It looks like just the same machine people have at home. And so I think the sense that employees know all that they need to know about their work machines, just exactly as you said, further creates tension in the workplace.

Leo: Well, and that's where, as much work as it is, additional work as it is, a really explicit policy that - and IT pros who take the time to explain why this is being implemented might help. I think employees, you know, they want to be good employees. They don't want to cause unnecessary trouble. They just don't understand what the issues are.

Steve: Well, one of the things that I have suggested, and we've talked about it, we touched on it briefly in the past under the issue of corporate monitoring of employee machines, is to literally, I mean, Draconian as it seems, put a couple-line message on the bezel of the display monitor on every single company machine that says, "This computer, which is property of XYZ Corporation, is subject to continuous monitoring and filtering of all activity; this is not your property," or something to that effect. I'd leave off the end part. But the idea being, it's like, look, make it very clear to users that this is not their property.

And then the other thing that I think makes sense, sort of as a safety valve, is a company could certainly set up, like, a break room or sort of the equivalent of an Internet caf where employees could take their laptops and plug into a secure and unfiltered, unrestricted network connection, the idea being that you have a break room or a coffee room or something, and IT could easily set up a router there that is not in the corporate network, that has no connection to the rest of the network in any of the machines or resources within the corporation, but just to allow users who want to check their personal email, who want to be able to use a laptop that they bring to work, allow them sort of a safety valve in order to access the network in a safe way.

Leo: It's that kind of creative thinking it's going to take, I think. You can't just be authoritarian and say, no, this is the policy, you know, shut up, you're an employee, do what we say. Because unfortunately, as much as you'd like to say that, I'm sure, employees will find a way around it. You've got to enlist their help. You've got to enlist their support.

Steve: And we've also sort of talked about, very much along these lines, how, for example, Hamachi could be used in a peer-to-peer fashion in order to circumvent some employee protections to allow people to potentially get themselves in trouble.

Leo: Yeah, we deal with that all the time. I certainly do on the radio show because all the time I'll get employees calling me, saying I'd like to circumvent these restrictions.

Steve: I mean, literally asking you how to get around these problems.

Leo: And, you know, I'm torn because, on the one hand, I'm on the side of users, and I want to say, yeah, you can. But on the other hand, and I usually try to do this, I also need to explain that, first of all, the law is in your employer's favor, the law is very clear, courts have always been very clear that employers own the hardware, they own the software, and

they can totally control what you do when you're at work. That's their property. So you don't have any rights when it comes to that. And furthermore, you could be risking your job if you start to try to get around these things. So I usually try to tell people that. But I sympathize, too, as a user. I'm no longer a user. I'm my own IT guy. But as a user in the old days I often chafed at those restrictions.

Steve: Yeah, well, and again, I think if there was some alternative that was reasonable, some way for example that, I mean, a corporate-sponsored solution like giving people a safe place that they can plug their laptops in that's protected. And it's like, okay, look, during the day this is what you do on the corporate machine. And if you want to take a break to check your email, lord knows what you want to do, but bring your own machine, your own laptop, and we will give you an isolated network that you're able to do this with.

Leo: Now, what about employees who have company laptops? That is a huge security risk because they bring them out into the unsecured open, and they can bring back all sorts of nasties.

Steve: Yeah, I mean, I don't see a good solution. There is an interesting technology which Microsoft has completed work on. There was something that they had for Windows XP that used to be called the Shared Computer Toolkit. Microsoft Shared Computer Toolkit for Windows XP was the full name. They've repackaged it and renamed it Windows SteadyState. I've begun to explore it as a solution for corporate desktops. It's sort of targeted more, its default configuration is targeted more to, as the original name implied, shared computer environment, for example like in a library or in an Internet caf when you want to essentially lock down a Windows-based PC so that anonymous and untrusted users can use the machine. And when they're done with it, it's basically anything that they did - and what they can do itself could be restricted. But the idea being that anything that happens is flushed out of the system.

Leo: Right. There are some third-party apps like that, too, like you might use it at a hotel. So you have a default setup, you know, the guy comes in, he's going to do - he's going to mess around on that computer. You let him mess around. But as soon as he leaves the machine, you reboot, and it goes right back to the default configuration.

Steve: Exactly. Exactly. And it turns out that, now, that would be a problem in your typical corporate environment.

Leo: Because you're destroying documents.

Steve: Well, yeah, exactly. But it turns out that, although it's not the default configuration, and it does require repartitioning, that is, creating another drive, because SteadyState is only able to return an entire drive to its original condition. But if you create another drive and put the user's profile information and desktop and documents folders there, then you can create a really interesting free solution which is protected from anything they do and won't execute code from this other drive, but still allows them to use it as their own workstation. So anyway, I'll be exploring that, and we're going to do at some point here before too long a podcast talking about the specific configurations of this. But it's an interesting notion for locking down a work machine so it's not absolutely restrictive, but it protects itself.

Leo: Right, right. Interesting, yeah. And, you know, we're on both sides. We're on the side of the user, but we also are very sympathetic, I think, to the IT guy who's got to deal with this.

Steve: Well, yeah. And I'm sure that our listeners probably find themselves on both sides, too, even if they're, you know, even with their own family or children, where they're trying to say, look, you just can't do this because it's going to infect all of our home network. I mean, after all, to some degree anybody with a router and multiple machines is a little environment that depends upon the security of each of the players within that community.

Leo: And that's the truth. That's the truth. Well, very interesting subject. I'd love to hear from our audience about what they think. Next week will be a question-and-answer session. That might be a good time to include your thoughts on this, and maybe your clever solutions, if you're an IT pro and you've found ways to solve some of these issues. I'm sure we'd like to hear from you.

Steve: Yup, GRC.com/feedback.

Leo: There you go. GRC.com is the place to go for Steve Gibson, of course, all of Steve Gibson, not only this show. And you can get 16KB versions there, too, by the way, as well as transcriptions of each and every show. But also all of his free security software, his very useful notes like the Perfect Paper Passwords series. And let's not forget SpinRite, world's finest, the best, the one and only, hard drive maintenance - and I'm going to underscore "maintenance" today - and recovery utility. It is a great program that everyone should have. GRC.com.

Well, Steve, I'm going to work on getting rid of this cold. It's almost gone now. I didn't cough once during the show, I think, so we'll see if I can do it in the next week. And I thank you for joining us. We'll see you next time.