Reducing Security Costs with Standard Configurations: U.S. Government Initiatives Transcript

Part 1: U.S. Government Background and History

Julia Allen: Welcome to CERT's podcast series, Security for Business Leaders. The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT working on security governance and executive outreach. Today I'm pleased to introduce Clint Kreitner, President and CEO of the Center for Internet Security. We'll be discussing recent U.S. government actions to require standard secure configurations for Microsoft Windows based in part on the definitions established by Clint's organization. So, Clint, thanks very, very much for making time today. I look forward to our conversation.

Clint Kreitner: Same here, Julia. I'm happy to chat about this with you.

Julia Allen: So, to get us started, would you please describe kind of your take on what the U.S. Department of Defense and Office of Management and Budget are now requiring for all government agencies and how this came about?

Clint Kreitner: What we're talking about, Julia, is a policy mandate that came out of the Office of Management and Budget that requires all federal agencies, by February 1st of 2008, to use a single configuration standard for all of their Windows XP and Vista systems. So the idea of enforcing a single configuration policy or image, if you will, on all of the hundreds of thousands — of millions, actually — of systems, the Windows systems in the government, is quite a profound development.

Another aspect of this particular policy mandate is that starting the end of June in 2007, all applications, all either custom developed application software or commercial-off-the-shelf packaged software, application software, will need to be demonstrated to be fully functional when running on a Windows XP or Vista workstation platform that is configured with these standard configurations. That also will be a huge help.

Julia Allen: So I take it that the impetus for this action was that so many of today's security vulnerabilities on major platforms like the Microsoft Windows platforms can be addressed by hardening or buttoning down or closing down aspects of the default configurations that are delivered. Was that the primary impetus for the initiative?

Clint Kreitner: It goes back, Julia, to 2002 at least, when the IA Newsletter, which is a Information Assurance newsletter put out by the Department of Defense, reported some studies that MITRE and NSA, the National Security Agency, had done to discover or identify the benefits of proper configuration and patching practice on the reduction of vulnerabilities. As you know, vulnerability reduction has been a key one of the 4 or 5 primary government policy principles way back since the National Strategy to Secure Cyberspace.

But NSA and MITRE ran some studies that went like this: (1) They took some Window systems out of the box, if you will, as configured by the vendor, which is basically non-configured, and they ran a popular commercial vulnerability scanners on them and identified the list of identified vulnerabilities; (2) then they configured these systems with the configuration settings in this applicable CIS (Center for Internet Security) benchmarks and then re-ran the vulnerability scanners. And they discovered that typically on the order of 90% of the vulnerabilities initially identified were eliminated by proper and competent configuration and patching practice. So that insight led to some developments in the whole process of improving configurations, which is really what CIS, the Center of Internet Security, is focused on since the early 2000s.

So in [the] 2004/2005 period, John Gilligan, who was CIO of the U.S. Air Force, decided to use the leverage of the Air Force's procurement of Windows systems to require that they be configured when delivered by Microsoft and its OEMs. He said, "The CIS benchmarking effort is producing very high leverage across the government and industry communities by providing the de-facto configuration standard for commonly used commercial products. Our (meaning the Air Force's) recently negotiated enterprise-license contract for over 500,000 desktops requires that Microsoft deliver its product compliant with the CIS benchmarks." And this is the prophetic part: "We are now planning to leverage this effort across the federal government." Well, that is what we're talking about.

Julia Allen: So it sounds like the Air Force action was really the first step toward setting the stage for what is now the Office of Management and Budget requirement. Is that correct?

Clint Kreitner: Exactly. The Air Force experience, if you will, the prototypical experience and starting with that requirement as [a] procurement requirement and then moving on through to the point now where the Air Force has 99-plus percent of all of its hundreds of thousands of Windows XP systems, Service Pack 2 configured in accordance with one single configuration image: that's an amazing accomplishment. And it's on the basis of that experience, that successful experience in the Air Force, that the recent OMB mandate is based.

Julia Allen: So, Clint, you started to say a little bit more about your Center's role, but how were these standard configurations defined both historically and how are they going to be kept up to date going forward?

Clint Kreitner: Well, it's been somewhat of an evolutionary process. In the early 2000s, in the early days of CIS, we fulfilled the role of gathering together users, security experts representing users from both the government public sector and also the private sector, and assigning them the responsibility of coming to consensus on how to best configure the various kinds of systems. And we're talking operating systems like Windows workstations, like Windows 2000, Windows XP, and now Windows Vista. We're talking about Windows Servers 2003, 2005. We're talking about network devices like Cisco routers and firewalls. We're talking about applications like web servers and SQL servers and the like. So that's the role that CIS has historically filled. And so that resulted in the Gold Standard back in 2002 for Windows 2000, and it was about around 2000, 2003 that the vendors began to realize that a large number of their very important users were engaged in this activity.

So they joined in the process, and we were very grateful when that happened. So now the technology vendors like Microsoft, like Cisco, like HP, like Sun, who are the purveyors of these software products or technologies that are being – for which configuration recommendations are being developed, they're very much in the game and they have been very helpful. One of the challenges you deal with, of course, is as you implement more and more of the security features on a platform, an operating system platform and middleware platform like a database platform, many applications cease to function correctly.

Julia Allen: Right, so you have that, basically that cost-benefit trade-off between being more secure and either reducing or allowing functionality.

Clint Kreitner: Right. And frankly the next frontier is that second part of the OMB mandate that I mentioned that starting at the end of this month, June 2007, any custom or off-the-shelf application software products that are run by the government need to be demonstrated to successfully and completely run in terms of all their features when installed on a platform that's hardened with the standard configurations.

Julia Allen: So, Clint, who is the owner of the configurations, and how is it envisioned that they're going to be kept up to date as time goes on?

Clint Kreitner: The answer to that question is NIST, the National Institute of Standards and Technology. It's all being gathered together in what is referred to as the National Vulnerability Database, nvd.nist.gov. And that site as a matter of fact is being redesigned as we speak, so it's a work in progress.

Part 2: Challenges and Tips for Implementing Standard Configurations

Julia Allen: So turning our attention to actually making this happen within an agency, what have you observed, Clint, are some of the challenges and costs of actually trying to put a set of standard configurations both in place and then keep them secure?

Clint Kreitner: Well, what the Air Force is doing I think is the model for doing that. They have developed these common configurations for Windows XP and Vista for the platform consisting of the operating system itself, consisting of Microsoft Office and Internet Explorer plus a small number of selected applications that will run, that will be fully functional on the platform that is configured in accordance with the standard.

And then beyond that, so in other words you have a standard software image for a Windows XP workstation or a Windows Vista workstation in the U.S. Air Force and you cannot deviate from that. They, as you may well imagine, they got tons of pushback from the system administrators in the Air Force that were administering these hundreds of thousands of systems, because their prerogative was being taken away and they were being replaced, their configurations were being replaced, the ones that they might have thought were the best ones were being replaced by a standard.

So there's a human aspect to enforcing this, and it takes a very strong will at the leadership level, which the Air Force has demonstrated very nicely. Without that leadership, will the pushback of, "Oh, this too will pass. Oh, we're different. This doesn't apply here. Oh, we've outsourced our operations. Oh, this is another un-funded mandate," – those kinds of pushbacks have to be dealt with in a resolute fashion by the organization involved.

But the idea is to have a standard software image for a particular platform, in this case Windows workstations, and then any additional applications that are installed on this system have to be tested to be fully functional on that standard configured platform in order to be brought into the suite of software that is included in that standard image.

Julia Allen: And then how are changes dealt with? Obviously new vulnerabilities are discovered, new versions of the software are released, service packs come down the road. How is that part of the process handled?

Clint Kreitner: Well, the vulnerabilities that are discovered on an ongoing basis are more of those vulnerabilities related to software defects, which are corrected by patching. So obviously up-to-date patching is part of this. The U.S. Air Force, I've heard a figure of like $200 million that they think they're going to save over a period of time by having standard software images where patches can be tested and applied globally on a centralized basis rather than the historical method of, "Okay, all you hundreds of thousands of users, here's a patch," and they all have to figure out whether to apply it and when to apply it and how to test it on a lab system so as to preclude the risk of bringing down a production system and so on. There's going to be a huge economic benefit to being able to do the patch testing and deployment on a centralized basis.

Julia Allen: Right. So it's one of those cases where centralization does give you a huge benefit over trying to handle this as a distributed problem.

Clint Kreitner: Absolutely. There's just no question about that. Just think about if you adopt this discipline, this configuration discipline, on a centralized basis that you have these standard configurations and you can — then applications need to be brought into the suite only to be brought into the suite, they have to pass through the testing gate. And then the final step in the Air Force plan, which is the last thing they're doing, is to enforce a universal comply-to-connect policy. In other words, if you attempt to log onto their network from a Windows XP or Windows Vista workstation, you will — that workstation will be tested for compliance with a standard software image for you to be logged onto the network.

Julia Allen: Well, that's obviously the ultimate enforcement mechanism, that you can't gain that network access if you aren't compliant, correct?

Clint Kreitner: Really, and of course that's been talked about on a conceptual basis for a long, long time. But credit goes to the Air Force for actually pushing this through to where they're on the threshold of being able to do that. Now they've done some very clever things; for example, they have made the laptops available on a discounted price basis to Air Force military and civilian personnel to take home and use as their home systems. So that if they are ever called upon to log-on to an Air Force, an official Air Force network from home, they're doing so from a system that conforms to the standard.

Julia Allen: And then would it be then correct to say by extension that the Office of Management and Budget program and their rollout to other federal agencies is really using the Air Force experience as the model?

Clint Kreitner: The memorandum from Karen Evans at OMB, who is the so-called e-gov czar within OMB, in her March 20 memo says this: "As a model for this effort" - this mandatory configuration effort in the federal government — "the Air Force uses common security configurations for Microsoft Windows XP." So very clearly the Air Force experience is explicitly being noted as the model for this new universal government mandate.

Part 3: Having the Collective Will to Make It Stick

Julia Allen: You've alluded to several actions about being resolute and having kind of the collective will to take this on. What would you say are the roles that governance and policy have played in bringing this about? You've also mentioned several policy actions, but any other thoughts along those lines from a governance and policy perspective?

Clint Kreitner: Well, a resolute commitment to doing this at the policy level, at the governance level, and at the operational leadership level of course are absolutely essential. Karen Evans, one of the reasons that Karen Evans is effective in her current position is that she was a system administrator at the Department of Justice way back some years ago when some hackers decided to replace Janet Reno's picture on the DOJ website with a picture of Hitler.

Julia Allen: Oh, my goodness.

Clint Kreitner: And so she got a baptism by fire early on in dealing with the consequences of improperly secured systems, and so she really gets it, she gets it. She understands the importance of configuration and patching. And so she has carried that understanding with her up the chain as she's moved up the chain in her career. And so it's very fortuitous that someone with that perspective is in the position that she is. So she was able to convince the head of the Office of Management and Budget, which is part of the Executive Office of the President, to begin this level of, based on the Air Force experience, begin this level of policy mandate government-wide, and so that (1) was crucial; secondly, having a model to use to prove to people, to the skeptics, that this was indeed possible and not just a pipedream was also crucial. So there was just a very fortuitous combination of circumstances: namely, Karen's outlook and perspective and the successful Air Force experience to convince the skeptics that this indeed was possible.

I've heard Ken Heitcamp [Air Force associate CIO for lifecycle management for warfighting integration], the individual who has been driving this Air Force effort refer to the resolute nature of the generals and colonels who dealt with the pushback and said, "Folks, stop your complaining. We're going to do this, and so get on board," and that was also essential.

So yes, policy, promulgation, governance, committed governance and committed leadership are all very, very key to doing this. Because let's face it, we live in the land of the free and we all like to think we have these enormous personal freedoms. And, by the way, one of them is freedom over what I do with my system, my computer, my Windows system. Well, we've discovered that unrestrained freedom on the part of the users and security don't mix very well.

Julia Allen: Right. I mean we're all so highly interconnected and interdependent that any one person connected can affect any other person or organization. So we really can't be autonomous when it comes to Internet and system connectivity.

Clint Kreitner: Exactly.

Julia Allen: So just to bring our conversation to a close — I mean, clearly, the Air Force has a particular culture. The U.S. Government Office of Management and Budget, the role that Karen is playing feeds into a particular cultural norm. How do you think or maybe what have you seen, in terms of adopting standard configurations, how that might have to be different for commercial and academic and other types of organizations that don't have a government or a military culture?

Clint Kreitner: Well, perhaps the polar opposite of the military culture would be the university culture, with which you're very familiar, where freedom is considered an inalienable right in all its dimensions. And so it's going to be very, very challenging in that environment to enforce this level of standardization and discipline. In between those two poles lie the average civilian government agency and average corporation. And the extent to which in those environments anyone [is] successful with this kind of effort is, I believe, very significantly tied to the will of leadership and the governance structure to make it happen.

Julia Allen: Right. But it sounds like there are clearly very strong cost-benefit arguments to be made that should make that appealing to at least consider.

Clint Kreitner: Absolutely. And there's all kinds of analogies for this. Southwest Airlines, for example, has been a very successful airline, and one of the components of its success that people don't think about very often is that they fly only one model of airplane, the 737. And so all of their parts, inventories, all the skills required of the maintenance people, and all of that can all be based on some standards that have proven to be very, very significant contributors to Southwest's ability to function and to be successful as an airline. So diversity, infrastructure diversity, creates its own problems. It creates some benefits, but it creates its own problems. So at least, I'm not saying that we need to all stop using Linux systems and Unix systems at all. I'm saying that within a technology like Windows, if we can standardize our configuration, standardize and centralize our patching practices, there are huge operational and economic benefits.

Julia Allen: Well, that makes good sense. Well, listen, Clint, I want to be respectful of your time and also just in closing do you have, other than the CIS website, which we'll include in the show notes, do you have any other sources you'd like to point our listeners to?

Clint Kreitner: The CIS benchmarks and tools are available free of charge at the CIS website. They're currently being downloaded at the rate of just a little over a million times a year internationally. And so I would just urge everyone to help themselves and to give us, shoot us an email or a phone call if we can be of help.

Julia Allen: Well, again, I'm so appreciative of your time and your expertise, and I think as a community we've benefited greatly from your personal and organizational commitment to bring this new initiative about. And I just applaud your efforts and look forward to seeing how it develops as we go forward.

Clint Kreitner: Well, thank you, Julia. It's always a pleasure to talk with you, and it's a journey. We and all of our colleagues are on this journey together, and it's not over yet.

Julia Allen: Excellent. Thank you, Clint.

Clint Kreitner: Thank you.