Dr. Unix runs into corporate security

Dr. Unix 21-02-2002

Since even a Dr. Unix has to make a living, I frequently sell my services to the needy. Not necessarily to the poor mind you, but to those in dire need of wisdom and guidance in the field of Unix and related pastimes.

At one of these customers (whose name shall be withheld for obvious reasons, but let's call them *BigAcme Corporation*) I was greeted one morning with flyers, distributed abundantly, stating that in line with BigAcme's security policy it was (amongst other things) no longer admissable for laptop computers of external consultants to be connected to the BigAcme intranet. Only systems "acquired and loaded with software through Authorised Channels" could legally be connected to the network. The flyer also contained threatening language with respect to procesuction, dismissal, sueing and the corporate death penalty.

At first sight this seems an extremely sensible and security enhancing rule. I mean, it's a well known fact that external consultants' laptops are infected with all sorts of viruses that are just waiting to jump over to their customer's networks. Like the consultants themselves, they should probably be sterilised and put in quarantaine for at least two forthnights before being allowed into the building. Stands to reason....

However, at second sight (and especially with some hindsight), "the owls are not what they seem..."

Most computer security experts will agree with me that, in the end, secure computers and networks occur when an educated and security conscious user population reacts wisely on any security related issues they are faced with. To assist users in making smart security decisions, a *security policy* contains guidelines on what is acceptable, and *security mechanisms* enforce and automate all or part of the policy.

However, real life has shown us time and again that mechanisms (like virus scanners, firewalls and authentication technology) are quite useless when users do not take security into account in their decisions on how to interact with the system. This security disregard can stem from lack of knowledge, lack of interest or (and this is the central statement in this article) because the security measures interfere with their wish to get their job done. No matter what your security policy states, or how many mechanisms you put in place, at the end of the day you are at the mercy of your users who can follow procedure or break it and employ mechanisms or circumvent them.

An important aspect that is often overlooked when implementing security is that **people want to get their work done**. This might sound strange, because given the Hobbesian creatures that we are, one might think that each and every obstacle that could be interpreted as a reason not to work would immediately be employed for that very reason. However, my experience has shown exactly the opposite: people want to get their assigned tasks done, and are more than willing to blow any (security) obstacle out of the water in order to get on with things.

Every security system that does not take this into account is doomed to fail.

So, in order to create an affective security environment, organisations would do wisely to keep the following in mind:

1. Do not engineer security as an obstacle; ensure that the secure way of working has low, or preferably non-existent, barriers.
2. Do not place the most important security decisions in the hands of users who are not capable of making them or who have too much incentive to break the rules.

So, for instance: to prevent people from sharing userids and passwords, make sure that the procedure to get a userid with suitable permissions is lucid, easy and **fast**. Or: configure your SSH environment so that a changed host key terminates the connection instead of asking the "Do you want to connect (yes/no)" question.

But, enough diversion for the moment. Let's return to BigAcme's new policy with regard to illegal laptop immigrants for a while. What could have been the reasons for BigAcme's security chiefs to impose this rule? I think their reasoning goes something like this: "*Laptops from non-BigAcme origin can contain software used to break into the BigAcme servers or to monitor network traffic. Furthermore, these laptop can contain viruses that can infect the rest of the network. And, even worse, these laptops can be used to download BigAcme corporate data and take it offsite.*"

First of all, I must admit that there are indeed some security risks involved in connecting "foreign" hardware to the network. However, if you think about the bigger picture, and calculate the risk of onboarding external consultants to do work on your IT environment, you would probably find that the risk posed by these consultant's laptop is negligible when compared to the related risk involved in giving that external consultant a userid on a production system. And another thought: is the risk of external laptops greater than that of BigAcme standard PCs that have been augmented with software by their legitimate user? (Which, although it is against BigAcme policy, is done regularly because it is next to impossible to get software necessary for one's daily work installed through Authorised Channels).

Let's first conclude that the new laptop security policy is not effective against malicious users who explicitly *want* to infect the network, monitor traffic or steal data. It is not hard to connect a laptop and hide it from view (e.g. in a desk drawer) or to employ regular BigAcme office hardware for these tasks. The floppy/CD drives in each BigAcme PC, the wide availability of tools to become local administrator (Windows NT) and the CD burners that are available in the LAN are really helpful for all that.

So, the real purpose of the security policy must be to prevent users from accidently hurting the BigAcme network from their laptops. About the only danger I find real in this case is that of viruses running on "foreign" laptops jumping over to the BigAcme network. And, if that is the problem we are trying to cover, I think there are much more effective ways to achieve this. Good virus scanners are one thing, but not giving ordinary users write access to executables and making them responsible for their (inadvertent) actions are certainly others that one might want to consider.

Another item worth mentioning is that this security policy is really hard to implement. Every intranet can be thought of as a star: at the core there are maybe hundreds of servers, then, going outbound, we find thousands of network switches, and at the rim are tens of thousands of desktop network connections. If you have a few vaults with valuable stuff in the centre of an office building, where would you post the guards? At each window and door? At each elevator shaft and corridor? Or next to the vaults? It is just not possible to guard each network connection, so every security policy or mechanism that expects only BigAcme hardware to be connected to the network would need rethinking anyway.

Another matter is that of barriers to delivering meaningful work. If BigAcme prohibits external consultants to use their own laptops, they obviously have to provide desk- or laptop systems for these consultants, because otherwise they're just blowing away the fees without reaping the benefits. Unfortunately, getting a standard BigAcme desktop system is a procedure that can easily take up to ten weeks. And if that sounds difficult, getting the network port at your desk to be patched into the intranet can be an almost insurmountable task. Before the no-laptop rule was decreed, I worked for weeks on my laptop with a local network hub (illegal, hence hidden from view by a bag), sharing one official network connection with my (BigAcme) co-workers. Getting 100Mb juice on the

unpatched RJ45 connector under my desk so far proved to be beyond the capacities of the local network administrators.

And even when a BigAcme LAN standard desktop PC would mysteriously appear, life would still be difficult. Like many contemporaries, BigAcme has a standard PC platform consisting of Windows NT (brrrr...), Microsoft Office and some other tidbits. The standard setup must be a secretary's dream, but it is unfortunately quite devoid of the tools of the trade of a Dr. Unix: no X server, no SSH client, no Java Development Kit, no VIM, no VNC, no decent FTP client, no decent browser, no decent tools... Getting these installed through Authorised Channels is a job for which there is simply not enough time in the universe. Installing these yourself is a) illegal, and b) not possible without breaking even more rules (because you are obviously not the local administrator of your own desktop PC).

So, what is the situation now that this new security policy has been put in place:

1. The network has not become any more secure. With over 60,000 office network ports worldwide, nobody will convince me that there are no "foreign" systems connected to the network any longer. I know for a fact that other business units of BigAcme do not enforce the rules in this respect.
2. A lot of external consultants are now restricted in their work, since they can not connect their laptops to the network, and do not have a BigAcme desktop PC allotted to them yet (which due to BigAcme's procedures can take many, many weeks). It is only a matter of time before their project leaders will instruct them to connect to the network again and get cracking!
3. I have spent three days finding a spare (and working) BigAcme owned PC and downloading and installing Rock Linux with all the amenities of life. This is stretching the term "Authorised Channels" a bit, but I think I can get away with it. Oh, and by the way, this desktop PC still uses the "illegal" hub to connect to the intranet....
4. A few people feel really good, because they have shown a firm hand in implementing security measures. They proclaim that BigAcme's network has become more secure. Meanwhile, BigAcme's real security problems stay unaddressed.

Well, that's progress for you. You can't stop it....

Other articles by Dr. Unix:

- Dr. Unix (pas très) hebdomadaire : des jeux de caractères, du symbole Euro (et des touches mortes)
- Dr. Unix (not so) Weekly: On character sets, the Euro symbol (and dead keys)
- Dr. Unix Weekly: Why Linux will replace most proprietary Unices
- Dr. Unix runs DOS and Windows programs on Linux

E-mail: Dr. Unix

[Index]