Controlling Vendor Access to Production Systems

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A reader wrote

>I am at present producing a standard on modem access by suppliers to our control systems. The control systems are used to control the electricity production process. I have just watched your CD on _Identifying and Managing IT Risk Factors_ and the security aspects of this relate to data-collecting office systems. While the CD did help formulate some ideas, it would be ideal to talk with someone who has looked into the security aspects of accessing control systems via a modem. <

Here is what I answered:

Thank you for writing to me. I do not know exactly what kinds of your systems need remote vendor access. For example, some of your process systems (generators? boilers? environmental controls?) may need access directly; your information technology systems (processors, mass storage, communications equipment) almost certainly do.

There are some easy policies and procedures you can define and implement at once. There are others that are difficult and expensive.

* Whatever you do, be sure that you eliminate canonical (i.e., uniform default) passwords -- that is, passwords that were assigned by the vendor and that are the same across all installations. Such passwords are notorious when users are unaware of the issue and simply accept what they're given out of the box. This component is essential and easy to accomplish.

* Modems used only for maintenance by suppliers (and thus never for anything else) should be disabled (powered down or even unplugged) unless and until they are required for a specific communication that has been authorized by the appropriate member of the operations team. When the task is over, the modems should be made physically inaccessible again.

* Going one better, use two passwords for vendor accounts: one known to the vendor and used only when access has been authorized; the other, unknown to the vendor, at all other times. Do not use the same access password across accounts. Ideally, use stronger authentication such as tokens or biometrics for all access to all systems.

* Verbal requests for authorization should include some mechanism for authentication of the request; e.g., use of a pass phrase recorded by both the vendor and the Ops team. E-mail requests for access should include the precise start time for access and be signed using a verifiable digital signature (e.g.,, Entrust, PGP, Verisign and so on).

* If it is feasible, you could arrange for more secure communications. For example, it is possible to install old-style encrypting modems and to give each vendor a matched modem so they and only they could use the dial-up communications link. The use of the link encryption is primarily to limit access rather than protection of the link itself against interception. The problem, of course, is the perfectly legitimate resistance your vendor will express to having to install a special, restricted modem tied to reaching your and only your site. I don't think you'll get much enthusiasm from your

own financial managers: this kind of pairwise or n-wise hardware-based access control is prohibitively expensive.

* A more practicable and useful approach is to use a remote access server (RAS) that provides encryption and access controls for anyone dialing into your systems. Such systems are useful for all your employees who need to communicate through the phone lines rather than through the Internet. You can usually install strong identification and authentication tools that will help you protect not only against abuse of your vendor access but also access by your employees and other users of your systems. Mind you, I don't imagine you have all that many people accessing your power plant computers from the outside, but RAS servers can easily serve multiple targets.

* Network topology is not always recognized as a potentially strong element of effective security. Details depend very much on the specifics of your functional requirements -- i.e., on who needs to access what in your networks. For example, in a real-time process-control system, it is possible that none of your production systems are hooked to any other systems that are in turn accessible through modems (or Internet connections). A general principle for secure network topologies is to segregate segments of your network that should not intercommunicate as a general rule. Perhaps in your case the example could be that there is no earthly reason why your accounting group should ever have any access whatever to the control systems for your generators. Such partition can be physical segregation (sometimes known as an air gap) of the networks -- no connection at all. However, there may be practical reasons for allowing limited access across parts of the internetwork; in those cases one can use routers and firewalls to limit traffic and allow only specified kinds of communication.

* A different approach is to discuss with your vendors whether they can function through an Internet connection. If you are already reachable via the Internet, then you can apply all of the security measures that are consistent with that medium: firewalls, virtual private networks, intrusion detection systems, token-based or biometric authentication.

>Do you know of any organization or website that might assist me?<

First of all, I will forward your entire message to my INFOSEC colleague in the nearest office of our company. As for other sources of information, you'll be in good company if you communicate with experts and other users through Network Fusion <http://www.nwfusion.com>, the SecurityPortal <http://www.securityportal.com>, and the ICSA.net site <http://www.icsa.net> among others.

Here are a few references to some recent articles located through the GaleGroup's ever-valuable _ComputerSelect_ database (see <http://www.computer-select.com>) that may help you with the most likely solution for your needs:

Computer Select, April 2000 : Titles -- Articles From Computer Periodicals

1. Getting RAS right for your network; Tests show pros and cons of NT-based RAS cards vs. lower-end dedicated RAS servers. Network World: Oct 11, 1999

2. Maximum RAS. Windows NT Systems: Oct 1, 1999

3. Insurer Goes From VPNs To Thin Clients In RAS Pilot. InternetWeek: Jul 5, 1999

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at
<mkabay@atomictangerine.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.