

DealersEdge

IT Security Issues in the Auto Dealership Environment

With

Grant Brosseau

*Director of Information Technologies
DeVoe Automotive Group*

Moderated by

Jerilyn Klein Bier

Editor, DealersEdge Business Briefings

Presented by DealersEdge

DealersEdge

Grant Brosseau has been in the automotive industry since 1974. He has held various positions within dealerships – including line technician, service advisor, warranty administrator, invoicing, service manager, director of fixed operations, purchasing agent and construction coordinator – prior to being promoted to Director of Information Technology in 1998.



Grant is certified in A+, Net+, CCNA Cisco, ISSP Security, MSCE and is Microsoft Office User Specialist (M.O.U.S.) certified (expert level, Excel). Grant has extensive hands-on knowledge of Windows Server 2003, Vista, XP, Exchange, Citrix, Spam Filters, Firewall, Router and Network Security. Grant holds a Bachelors Degree in Computer Information Systems with a minor in business, and a Masters Degree in Management Information Systems. Grant served on the National Information Technology symposium panel, is the chairman of the NCM Automotive Information Technology 20 Group, and has been nationally recognized in *DealersEdge* publications and a Southwest Florida business magazine for innovative technology practices in the dealership environment.

DealersEdge Audioconference System / Network Security

Designing a secure network begins with a written plan that is evaluated and accepted by Senior Management. I know what you're thinking, "What does Senior Management have to do with it?" The answer is plenty. Everyone needs to support the common cause of network security and corporate policy that bind it along with associated cost. Security planning isn't easy and has several steps:

- Planning your corporate security policy
- Evaluating the risk of losing information, unauthorized access
- Evaluating the risk for different information categories and servers
- Evaluating the cost – both financially and public trust
- Staff knowledge and training
- Corporate response to security breach
- Evaluating current hardware and design
- Equipment scalability
- Balancing risk to cost
- The security plan is never final, it is always under review and evolving with technology

Until a few years ago, network security was often looked upon as unnecessary because the thought was, "This is just a car dealership, not a bank. We don't have anything anyone would want." That statement is farthest from the truth and has nothing to do with bank account numbers or free services obtained. It has to do with challenge, random hack discovered by automated port scanners, theft of consumer information, and illegal use of your servers for hosting illegal sales that trace back to you. It could also lead to acts of terrorism by using your equipment to launch cyber attacks and viruses against computer targets in this country or other businesses. This could lead to litigation – not to mention costly damage to your reputation when a customer is notified under privacy laws that your network security has been breached and customer information has possibly been stolen.

This is all very real and by no means a scare tactic. Dealers need to defend themselves and their years of investment and reputation. Reputations can take years to build and seconds to destroy. So how do you defend against something you cannot see? How do you defend against an enemy on the other side of the world or in your neighborhood 24/7? Security! Don't think of security as just another expense, think of it as insurance and your exposure to the various types of risk that come with a security breach. Your best line of defense starts on the outside and works inward so let's talk about the components that should make up this line of defense.

Edge Router

The Edge Router is exactly as the name implies. It resides on the edge of your network between the internet and you. It defines the edge of the world (public address) and your network (private address). The Edge Router typically has your public address and translates it into your private network address. Filtering or access rules can be assigned to this device to help enhance security. This single component should never be your business network's sole device. This design is typical of home users that use high speed services. They are provided with a router/modem that provides access to the internet via a single component. Once this device has been breached, the perpetrator is inside your network. This is the first line of network defense and should be coupled with other network devices. The Edge Router marks the outside edge of your demilitarized zone (DMZ).

Firewall

Firewalls come in many assorted flavors and have the ability to analyze incoming and outgoing information (packets). If you have used the internet for any length of time, you have probably heard of them usually in a sentence saying, "The firewall won't let me in or out." Basically, consider a firewall as a barrier to keep intruders out of your network. Firewalls use one or more of three methods to control packets flowing in and out of the network.

- Packet filtering – small blocks of data (packets) are analyzed against a set of rules or filters. If the packet doesn't meet the criteria, it is discarded.
- Proxy service – information from the internet is retrieved by the firewall and sent to the requesting machine.
- Stateful inspection – compares key parts of the packet to a database of trusted information. Outgoing packets are examined or monitored for specific characteristics. The incoming reply packet is compared for specific characteristics for a reasonable match for authenticity and then allowed to enter.

Firewalls usually have an external and internal interface that would have different addresses. The outside address would be the same as the inside address of the edge router. The inside address of the firewall should carry a completely different address and often is different from your private network address.

Firewall cost can vary extensively and have the ability to filter on different layers. When purchasing a firewall, you must consider how it fits into your network security plan and comfort level of risk, as well as the ease of administratively managing it.

Create your DMZ with Depth

What is a DMZ? Thinking in terms of military terminology, a DMZ is a demilitarized zone or a buffer between lines. In the world of information technology there is a 24/7/365 war raging outside your edge router that separates your network from the world. The

amount of devices information (packets) must pass through before they enter your private network defines your DMZ and depth.

The primary role of a DMZ is to mitigate risk of unauthorized network access. The DMZ accomplishes this by providing network level protection by segmenting the public network (internet) from your private infrastructure. The illustration below (Fig. 1) is a typical DMZ architecture. It is often thought if your network has a firewall you are secure – not true.

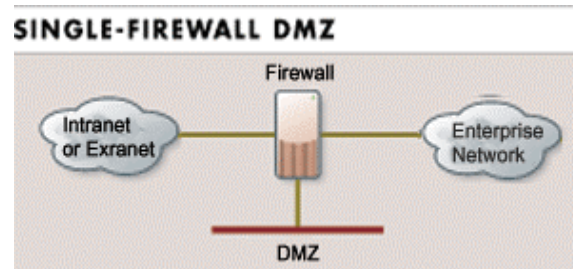


Fig 1.

Defense in DMZ depth is the process of layering defenses to provide extra protection. By increasing your depth, you increase the cost of an attack. The cost of an attack is not totally measured in dollars but also in time invested. Look at it as the only house on the block with a security system. A would-be attacker would rather enter as many unsecured homes as possible rather than invest the time and effort to access the secured home and risk possibly getting caught. The multi layers of deep DMZ help prevent direct attacks against sensitive data and make network reconnaissance difficult for the intruder – plus the implementation of intrusion detection, honey pot or glass house will buy you time to detect and respond to a DMZ breach.

As more devices are added prior to entering the private network, so does the depth of the DMZ increase – hence increased network security. Typically, a DMZ will carry a completely separate network addressing scheme from the private network. This separate network addressing tactic is designed to confuse the attacker performing reconnaissance. Often you will find a web server and or mail server residing in this zone.

Network Switch

Network switches can be assigned network addresses to divide or split networks. To simplify the complexity of switch programming let's say switches can be extensively programmed similar to routers. The purpose of adding a switch would be to split / segment your DMZ.

Internal Router

The internal router is the inside definition of your DMZ. It is at this point the DMZ addressing is translated once again to the private network. The internal router is

responsible for sorting out packets of information looking to find their way out to the internet via firewall or to other routers within your network. The internal router also can be programmed with more filters rules.

Conclusion

Network security is different for everyone because everyone has different values and lives with different levels of risk. Consider car or homeowner insurance: it's all about the comfort level of risk. Network security doesn't mean you will never have a security breach, it means it will be more difficult for a breach to occur. Doing nothing is just waiting for disaster, being proactive and staying proactive is defensive.