Just going with the Flow

Andrew Yon IV posted Jun 19, 2024 23:12 Subscribed

Ok so a firewall is a wall that will prevent undesirables that is easy to block based on identifiable properties, like protocol or port. However, one man's trash is another's treasure applies to traffic much the same way, so no one size fits all is available for something as in depth as security. An easy example of this is to think of the data as international traffic, yes that's what it is on the internet, but I need you to instead think of the traffic flowing through checkpoints at a country's borders, especially one that is involved in military actions against a neighbor because that's just like the internet too.

A firewall actually doesn't keep everything out like a fence or moat, it regulates what gets past it, like the Customs agents screening luggage and passports at the airport. A firewall checks the ports (Reason for entering the country) and the protocols (Nation of origin and any recent visitation stamps to other countries) and then waves them on through. Once it is inside, the IPS or IDS becomes the local cops and they have the means and authority to stop and search someone more in depth like checking out who they are meeting with and even checking their luggage (internal IP destination and packet sniffing). If they find something suspicious they can then do a more thorough investigation of what is going on and possibly even arrest or deport the individual (full packet interception, block the IP address, and pass the information along to authorities as recovery/prevention measures are taking place).

I think of firewall policies not as a protective method, because all protections

have a work around, but a limiter on what fights I am willing to fight, and what vulnerabilities I will need to expose so I can do what I want to do. If you are running a network that doesn't need FTP or VoIP, close those ports off by all means, it's best not to have to fight against attacks that you do not absolutely need to. This will allow you to focus more on detecting the known work arounds for what you have to allow in, and since most of those can be fixed with an update to software, maybe it can give a little time to find the unknown exploits. Dynamic IDS/IPS devices can scan for the known ones, that gives you time to filter the alerts on those kinds, and frees up even more time to look at the anomalies to determine if there is a possibility that one of them may be a threat.

The real key to anomaly detection comes from knowing your traffic patterns and usage demands (protocol, loads, frequencies, and if possible users) of desired traffic. If your company is successful enough to be growing (best kind to work for) you demands will change and so must your protections. However, since most successful attacks take days or even months to successfully pull off, the threats themselves have probably already worked their way into your approved logs or even regular traffic patterns and restore points. As such policies and practices should be as dynamic as the threats that they are in place to prevent. Part of the preparation any detection of a threat, and a restore point creation should include the following: 1) setup an isolated sandboxed network. 2) install the restore point. 3) remove the threats from the restore point. 4) create a restore point from that system status. 5) harden the firewalls and IDS/IPS settings. 6) perform a cleaned install from the restore point. 7) field phone calls from the loss of a few hours worth of work, "No, I haven't forgotten that the printer is out of ink on the 5th floor, I have changed your settings please go get your print out off of the printer on the second floor. Would you like me to approve all 50 of the requests you sent to the printer que, or do you just need one?".

Alternatively, do a dynamic restore by removing the threat during normal slow traffic periods, holidays or normal vacation times for internal systems, and build a second web-front database from the cleaned files in a sandboxed setup. Flip the switch on which server the new requests are coming into, and then clean the threats from the first. After the new database creates its restore point go

back to the isolated network, import the new restore point, add the data that was generated on the original and now cleaned server. Keep the isolated system running as an emergency switch over by using it as a live testing ground for threat detections and possible network or application improvement tests.

DOCUMENT EVERYTHING. Some regulations makes it illegal to tamper with restore points for certain industries (financial as an example) and what records are tampered with (tax records, accounting, emails). If possible make a tamper resistant (CD/DVD) backup of any files that are being removed and why in a text format note on the infected backup media, along with the infected restore point with a warning notice about the infection, I suggest red sharpie on a yellow sticky note. It will work as a shield and evidence at the same time. If done properly it can be used as evidence to prosecute someone. If done properly it will be a shield to protect you during the actual investigation to determine the one to be prosecuted. However, an physically locked and encrypted USB drive can be used for rapid evidence provision in case they do not want several TB worth of DVDs.