Don’t WannaDie: Using a Zero Trust Approach to Secure Healthcare

Christopher Frenz

AVP of Information Security

Interfaith Medical Center

Mock Mass Malware Outbreak

- Made use of the EICAR test file

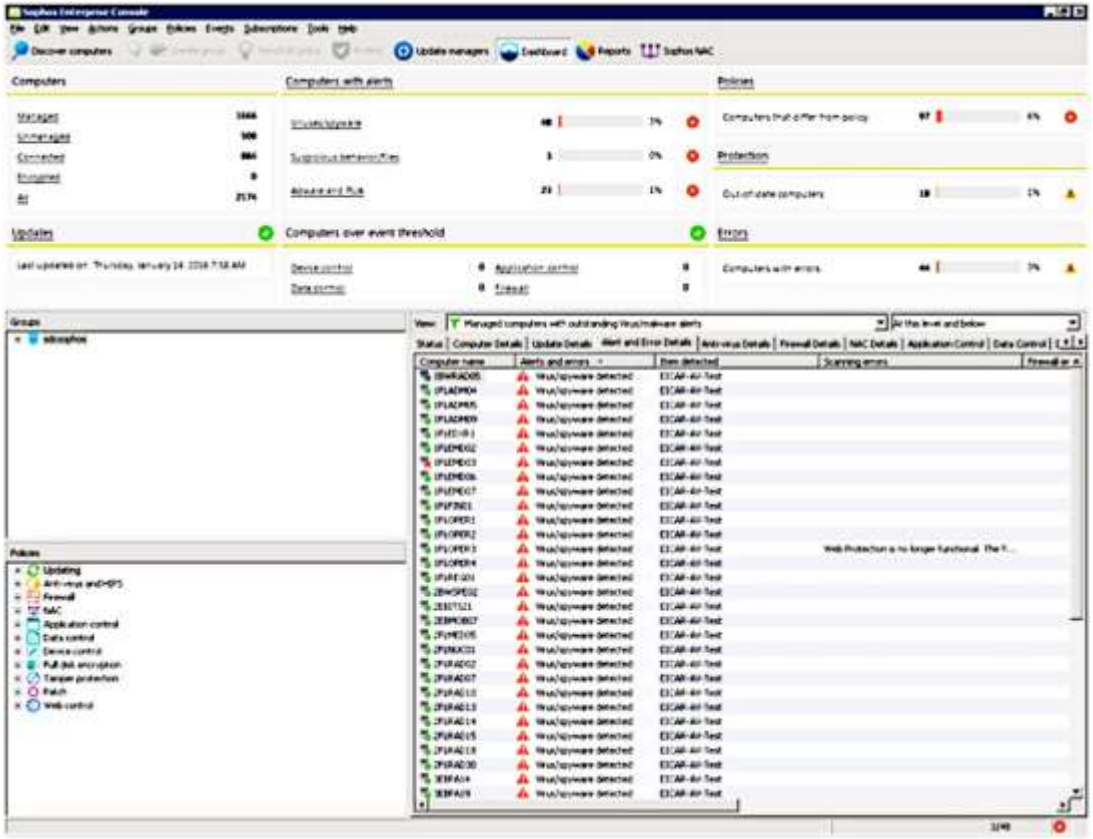
```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

- A harmless file that all AV makers recognize as a virus for testing purposes
- Wanted to evaluate:
  - How well our AV software was able to detect the outbreak
  - How quickly staff would identify, respond to, and contain the outbreak

Simulating the Outbreak

- Wrote a Perl script that accepts a listing of all computers in the organization
- It was setup to copy the EICAR test file to each PC on the list and execute the file to set off the AV
- Script was executed without the knowledge of other staff members to get a realistic evaluation of real world response

During the Outbreak



The Good

- IT staff members did identify the outbreak, track down the source of the infection, and remove it from the network
- Many in place security features stopped the spread of the infection to parts of the network (some examples):
  - Network segmentation - ACLs between VLANs
  - Security configuration of our VDI desktops

The Bad

- While the incident was detected and contained response time could be improved
- No normal users reported anything to the help desk even though AV infection prompts appeared on their desktop at the time of detection by AV

Lessons Learned

- The configuration of our AV software was updated to make the outbreak more noticeable to IT staff
- Internal training was conducted to better improve the ability of IT staff members to detect the source of such an incident and how to handle it
- IT staff members now better understand the need for certain security practices
- Based on the results of the test we are able to further harden the security of network infrastructure and endpoints – enhanced network segmentation to move towards a zero trust model

Zero Trust

- Zero Trust – enforces the creation of a perimeter around every network enabled device to ensure that only preapproved traffic flows are allowed

- Zero-trust environments and the high level of network segmentation they require are an ideal way to help mitigate the spread of malware and other security threats because communications between systems on the same network will likely not even be possible unless there was already a legitimate use case defined in the firewall polices that control the communications between systems.

Steps to Zero Trust

- Identify all information systems
- Identify data flows between information systems
- Implement network segmentation
- Test your setup with simulated incidents/red team exercises

Where is all my Data?

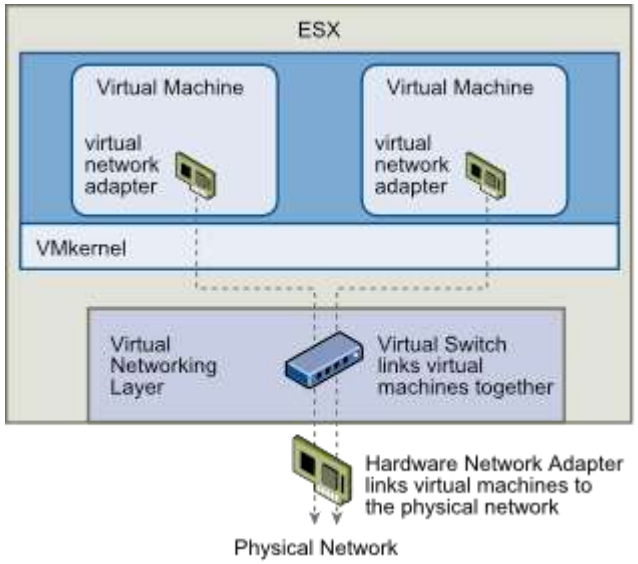
- Organizations should have a map of where all of their data assets are and where their data flows to
- This effort needs involve more than just IT. A surprising amount of sensitive data may not be under the control of IT (HR, Finance, etc)
  - Finance sending data to an external vendor for revenue cycle management or collections
  - Paper based records such as a morgue logbook may still have PII
  - Shadow IT, BYOD, etc
- This map should include data collected and distributed by IoT devices like security cameras, medical devices, etc.

Data Flows

- Interviewing the system administrators to see where data comes from and goes to
- Manufacturers documents to see ports and protocols
- Collecting and analyzing NetFlow data
- Vmware Vrealize Network Insight
- Wireshark
- Identified data flows can be used as the basis for network segmentation and zero trust

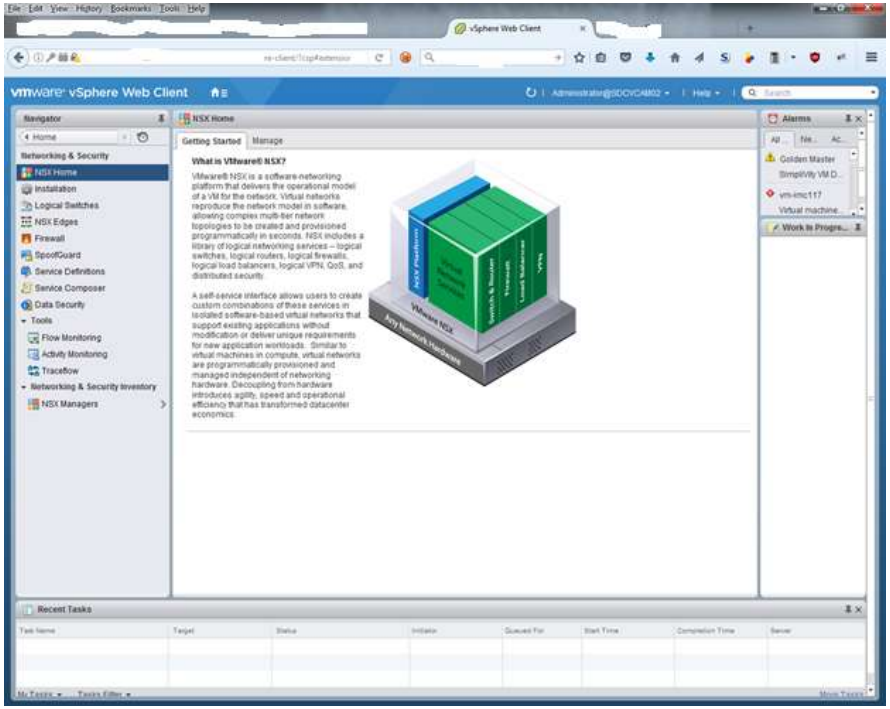
Virtualized Environment Challenges

- Virtual environments were traditionally harder to secure with network access controls as communications between virtual machines on the same host often occurred on the back plane of a server and never reached a switch or other network appliance



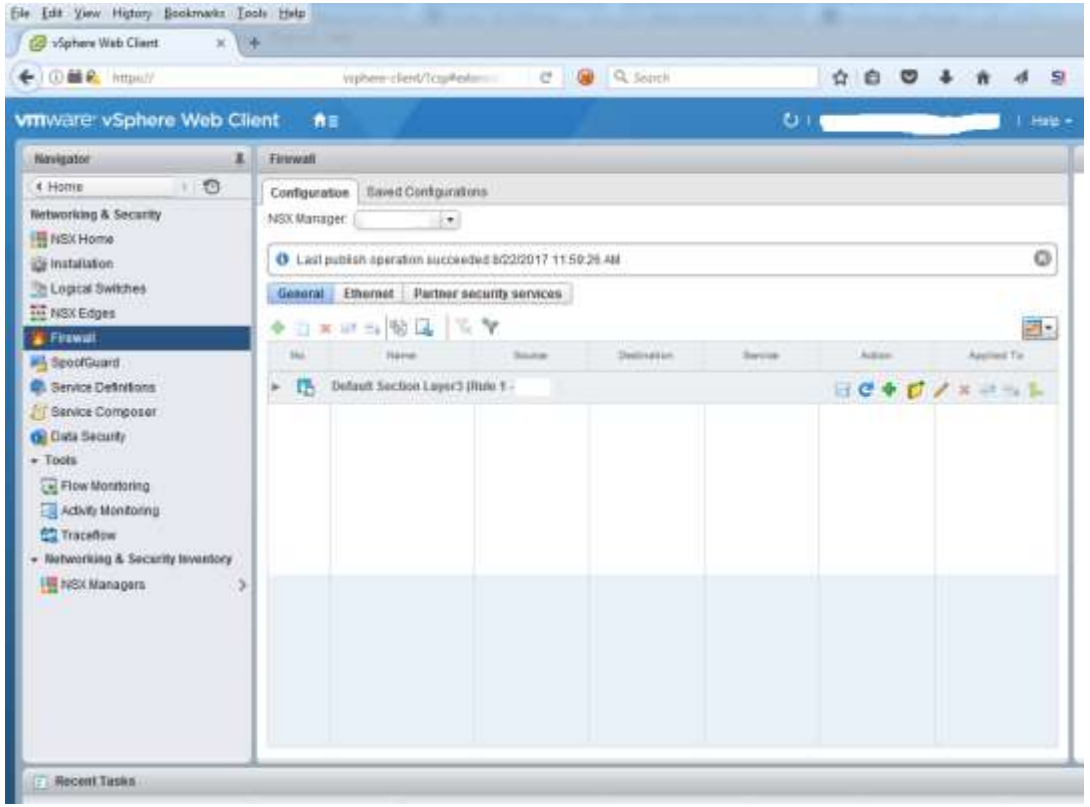
Zero Trust for Virtual Environments

- Software Defined Networking and security products like NSX and Hyper-V network virtualization make approaching zero trust networks more feasible



Zero Trust with NSX

The Distributed Firewall allows for each virtual machine to have a perimeter formed around it and for rules to be configured in the firewall to control communications to and from the virtual machine



Where to Start

- Start with the most widely accessed systems with the most well k
  - DHCP
  - DNS
  - NTP
  - Web Ser
  - KMS

Systems requiring more specialized rules or more thorough isolation can be added over time

No.	Name	Source	Destination	Service	Action	Applied To
	WSUS	10.	S .	TCP:...	Allow	Distrib...

Physical Network - NAC

- Make use of NAC to create port based polices that restrict communications based on device type.
  - E.g. – PCs are allowed to connect to the subnet containing the EHR and PACS systems, but are not allowed to communicate with each other
- NAC based policies created for other device types such as printers, security cameras, etc
- NAC works well for devices types where there are a large number of devices with common access needs spread out across the organization
- Can control communications between devices plugged into the same switch

Internal Firewalls

- Internal firewalls are also used to control communications between subnets and to control communications between one of a kind devices that are on the network – e.g. an MRI machine

Repeat the EICAR Mock Incident

- Only the endpoint the script was launched from was impacted as the endpoint was prevented from connecting to other endpoints in the organization

Real World Medical Device Incident

- X-ray machine software image install disk came infected with Conficker

Questions

- https://www.linkedin.com/in/christopherfrenz/