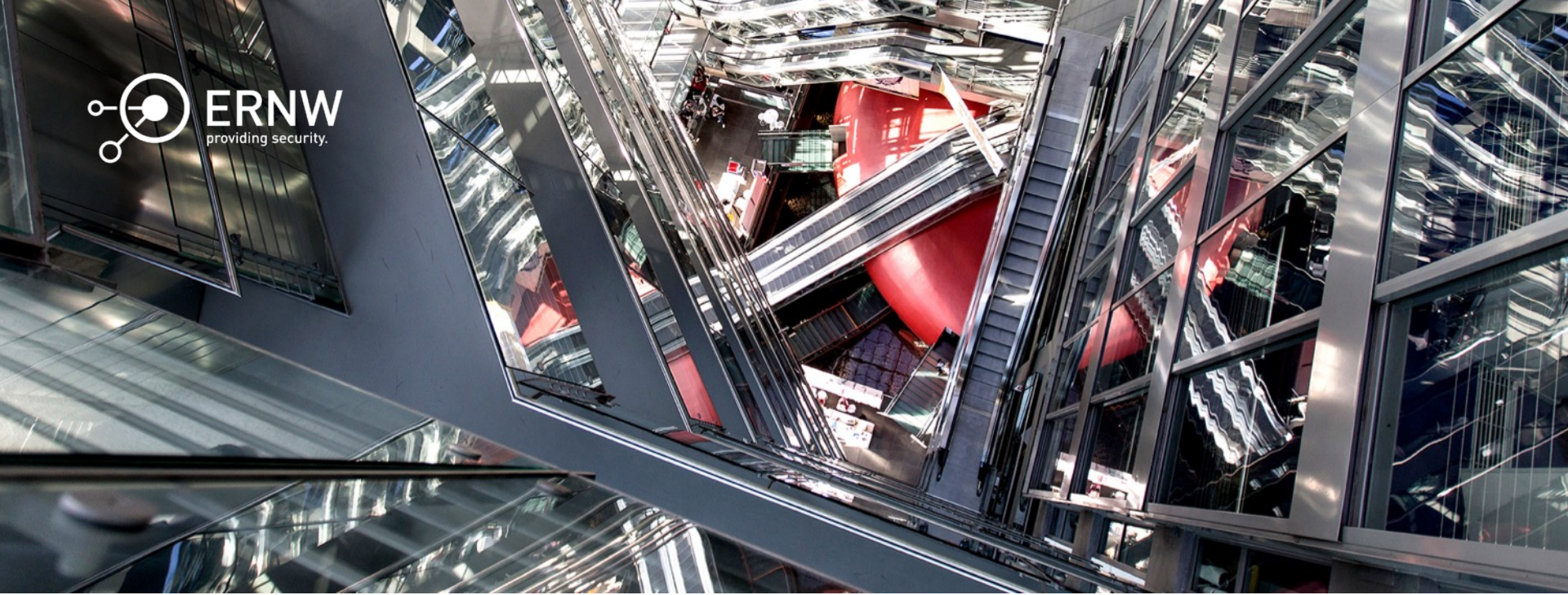


Doing the same thing over and over again: A Critical View on Security Products

Matthias Luft, mluft@ernw.de, @uchi_mata
ERNW Research GmbH

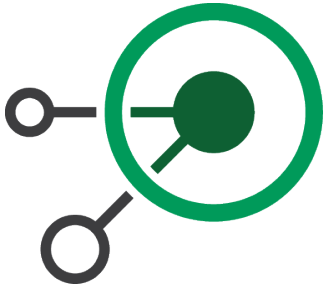
ERNW
providing security.

ERNW

- Vendor-independent
- Established 2001
- 60 employees, 40 FTE consultants
- Continuous growth in revenue/profits
  - No venture/equity capital, no external financial obligations of any kind
- Customers predominantly large/very large enterprises
  - Industry, telecommunications, finance

ERNW
providing security.

Since 2016



ERNW
providing security.

ERNW
RESEARCH
pursuing knowledge.

ERNW
INSIGHT
expanding your knowledge.

ERNW
providing security.

Agenda

- Defining Security Products
- Shortcomings & Marketing Gaps
- Alternative Approaches

ERNW
providing security.

Security Products

- Obviously, software that performs security functionality or implements a security feature.
- Security Product vs. Security Appliance

ERNW
providing security.

PAN-OS Architecture

- 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

- For
- Runs **FortiOS** - based on Linux.

ERNW
providing security.

Special Vulnerabilities?

- Why are security appliances/products special when it comes to vulnerabilities?

ERNW
providing security.

ERNW
providing security.

Special Vulnerabilities?

- Why are security appliances special when it comes to vulnerabilities

  Very high complexity & Lack of verification

- The first due to the nature of their task,
- The latter due to inherent trust for security products in many environments.
  - Lack of understanding for *Feature vs. Level*

Special Exposure

- Designed to process untrusted input!
- Think of…
  - IDS/WAF/$ALG: Untrusted Internet traffic
  - AV: Untrusted files
  - Advanced Threat Protection: Untrusted files

ERNW
providing security.

Relevant Vulnerabilities

- 2015, FireEye MPS, multiple RCE
- 2015, Kaspersky Antivirus, RCE
- 2016, Cisco ASA, RCE
- 2016, Palo Alto Networks NG-FW, multiple RCE
- 2016, Symantec various products, RCE

- List is (by far) not complete.

ERNW
providing security.

Vulnerability Details

- 2015, FireEye MPS
  - Authenticated web command injection
  - ZIP Symlink Unpacking Vulnerability
  - Buffer Overflows in Network Monitor
  - No DEP, PIE, stack cookies
- 2015, Kaspersky Antivirus, RCE
  - Several file parsing vulnerabilities
  - No Stack cookies, no sandboxing
- 2016, Cisco ASA
  - Buffer Overflow in SNMP processing
  - Linux-like platform
  - No exploit mitigation techniques at all

ERNW
providing security.

Marketing Gaps

- **Real-Time protections** – The IPS Software Blade is constantly updated with new defenses against emerging threats. Many of the IPS protections are pre-emptive, providing defenses before vulnerabilities are discovered or exploits are even created.

Products

FireEye cyber security products combat today's advanced persistent threats (APTs). As an integral piece of an Adaptive Defense strategy, 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. View the FireEye Corporate Brochure to learn more about our offerings.

ERNW
providing security.

A Word on Signatures

- Signature in the traditional AV sense: Checksum over (part of) a file.
- Or, more general: static description of attributes of a file/entity
- “Behavior-based analysis”:
  - Generating an execution trace (files, registry keys, network connections)
  - Match certain patterns in this trace
  - => Static, even though evolved, signature of an entity.

ERNW
providing security.

Make Assessments Possible

- From https://blogs.oracle.com/maryanndavidson/entry/no_you_really_can_t

'This is why I've been writing a lot of letters to customers that start with "hi, howzit, aloha" but end with "please comply with your license agreement and stop reverse engineering our code, already."'

'[...] there are a lot of things a customer can do like, gosh, actually talking to suppliers about their assurance programs [...]'

ERNW
providing security.

Contrast

- F-Secure's Vulnerability Reward Program:

"You may reverse-engineer and decompile F-Secure clients strictly and solely for the purpose of conducting security research for this vulnerability reward program. [...]"

Can you provide a vulnerability history of your solution?	XXX does not disclose this information.
Can you provide your guideline for security systems development/documentation about your Secure Development Lifecycle/Secure coding guidelines?	XXX development teams follow a proprietary software development process that includes security as a key component given that the product operates in demanding security environments. XXX development process includes: design reviews that include security review, code verification using static and dynamic testing tools, code reviews with peers and architects, significant Quality Assurance (QA) testing that includes testing for security issues, and finally system testing that includes vulnerability scanning.
Can you provide a report of a recent security assessment of your solution? The report can be redacted where necessary or complemented by the documentation of the lessons learned/steps of mitigation.	No, XXX does not disclose this information.

ERNW
providing security.

Measurable

- Cyber Independent Testing Lab
- Common Criteria (to a certain, test laboratory-dependent) extent
- ERNW's 2010 Security Rating of Closed Source Software

- => Requires also a certain need to complete those metrics.
- We can also provide input on (security) product evaluation metrics we used earlier.

ERNW
providing security.

Vendor Trust

- Trust without evidence is faith.
- Any vendor documentation requires trust.

ERNW
providing security.

Vendor Trust

- Symmetry & Transparency
  - Why trust a vendor with your data that doesn't tell you whether they use ASLR?
- Consistency
  - How many vulnerabilities have been there in the past?
- Integrity
  - … and were they handled in a fair and open way?
- Competence
  - Are they engaging in the research/security community?

ERNW
providing security.

Conclusions

- Understand security features vs. security level
- Provide clear development requirements
- Require vendors' commitment to trust-enabling behavior

ERNW
providing security.

Thank You For Your Attention!

Critical Questions?

mluft@ernw.de

@uchi_mata

www.ernw.de

www.insinuator.net