How White Hat Hackers Operate

Andreas Falkenberg, Senior Security Consultant,
SEC Consult Deutschland Unternehmensberatung GmbH

About me

Andreas Falkenberg, M.Sc.
a.falkenberg@sec-consult.com

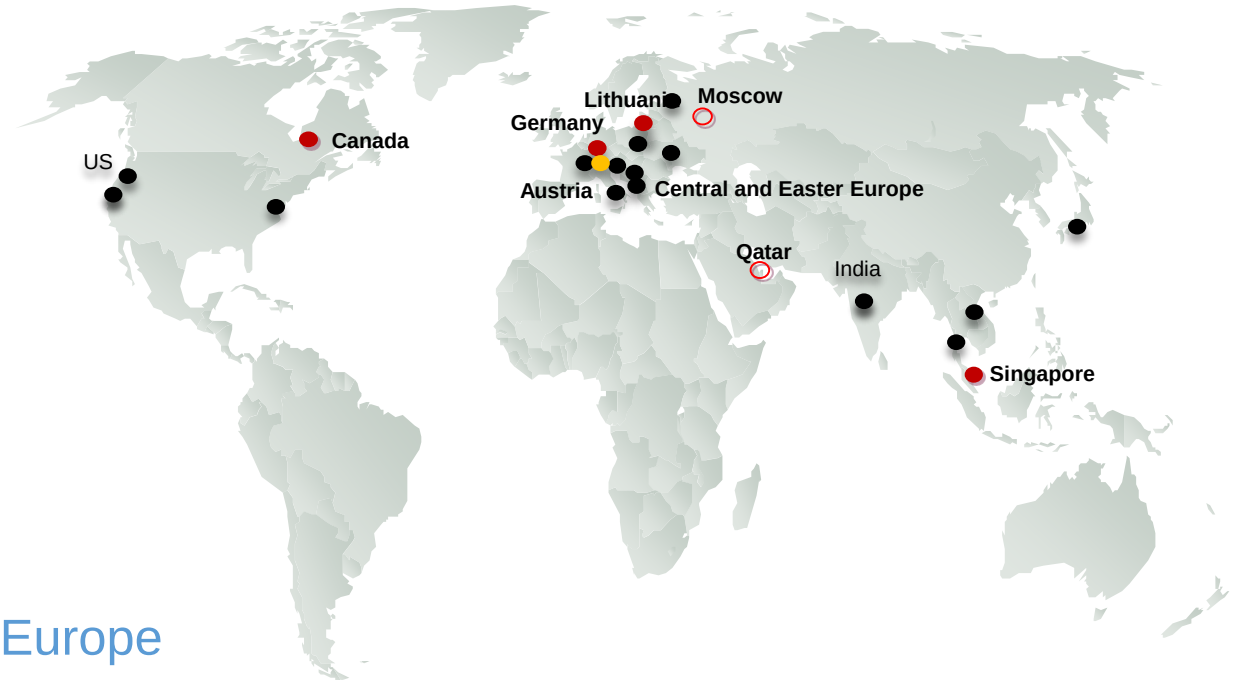
- Security Consultant @ SEC Consult
  - Source code audits
  - (Web) application penetration tests
  - Internal / external network audits

- Speaker @
  - OWASP AppSecEu 2011, Dublin, Ireland
  - IEEE ICWS 2013, Santa Clara, CA, USA
  - ISACA Chapter Meeting, August 2014, KL Malaysia
  - Lecturer FH Technikum Wien, AT
    - Web App Security SS 2014,
    - Web App Security WS 2014/2015

SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

SEC Consult in a Nutshell

- 50+ White Hat Hackers
- ISO/IEC 27001 certified
- Delivery Centers in
  - Austria,
  - Germany,
  - Lithuania,
  - Singapore,
  - Switzerland
- strong customer base in Europe and Asia
- Established 2002



SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

SEC Consult in a Nutshell

- 50+ White Hat Hackers
- ISO/IEC 27001 certified
- Deliver
  - Austr
  - Germ
  - Lithu
  - Singe
  - Switz
- strong customer base in Europe and Asia
- Established 2002

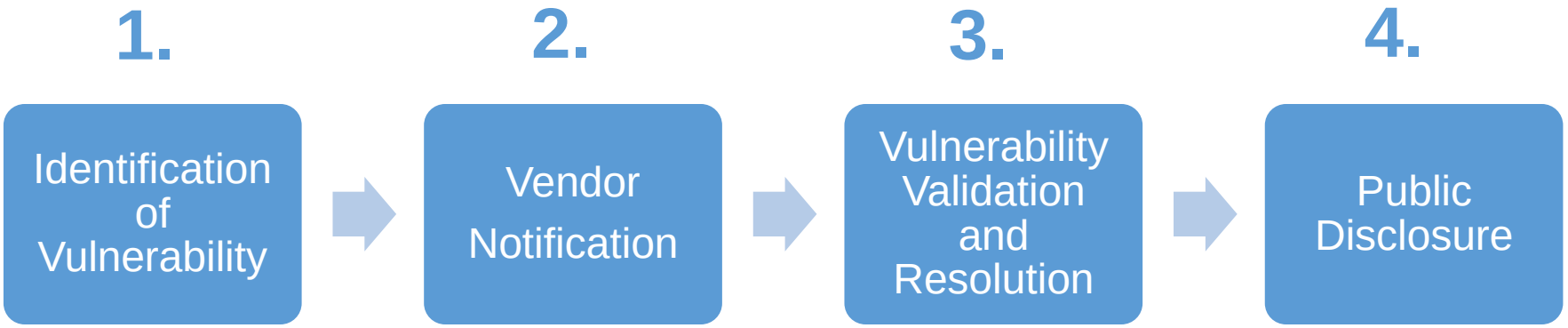
White Hat Hackers find…

- REAL vulnerabilities in…
- REAL software and disclose them responsibly.
- REAL consequences are the result if those vulnerabilities are exploited!

SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Responsible Disclosure Process

Responsible Disclosure



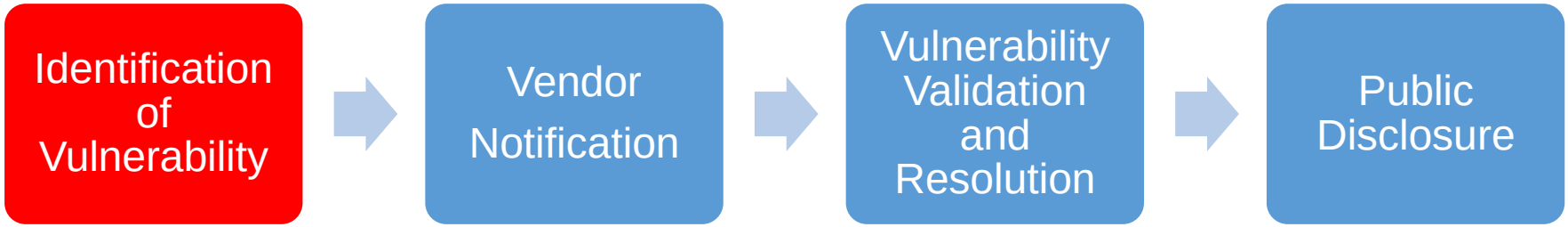
… A defined process on how to publish vulnerabilities

…"*rules of engagement*" for White Hat Hackers.

Identification of Vulnerability → Vendor Notification → Vulnerability Validation and Resolution → Public Disclosure

- Be creative!
- Be confident!

- In Capture the Flag Events
- In Courses at University / School
- @ **SEC Consult**
  - In Customer Projects
  - As a Researcher

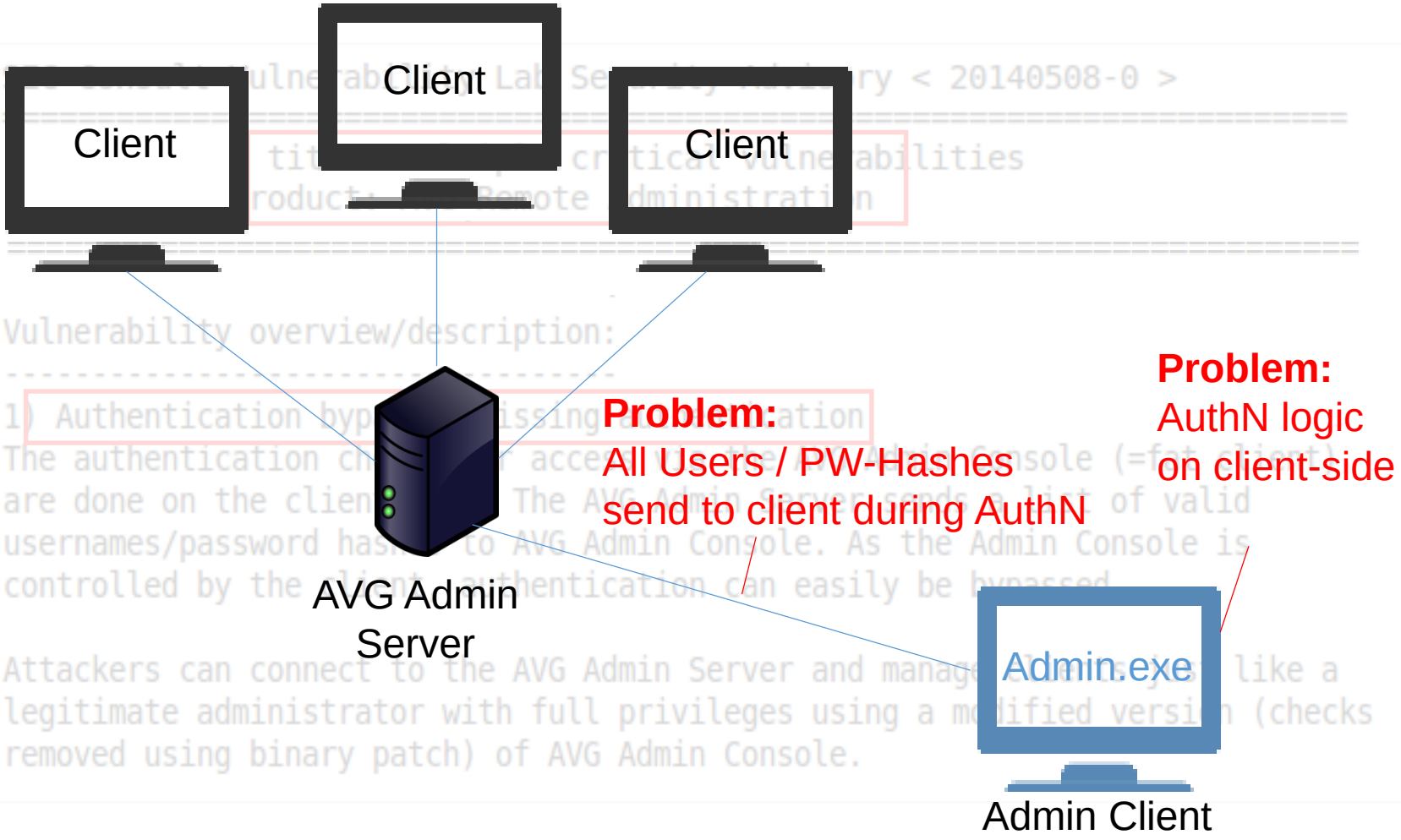


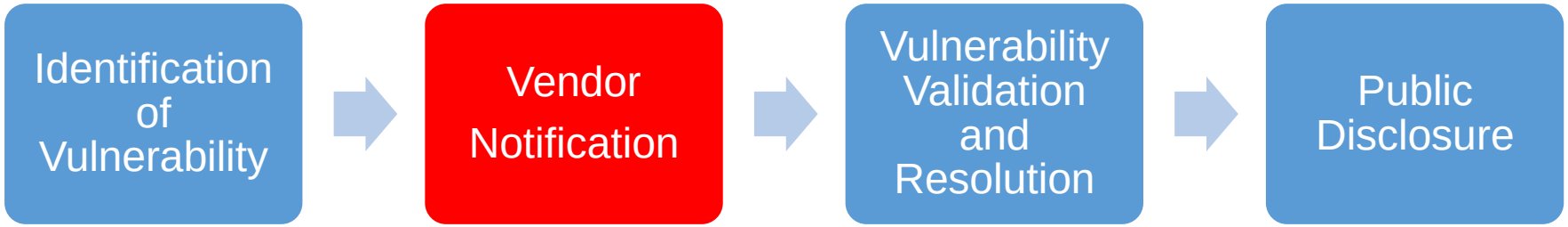

```
SEC Consult Vulnerability Lab Security Advisory < 20140508-0 >
================================================================================
               title: Multiple critical vulnerabilities
             product: AVG Remote Administration
================================================================================

Vulnerability overview/description:
-----------------------------------
1) Authentication bypass / Missing authentication
The authentication checks for access via the AVG Admin Console (=fat client)
are done on the client side. The AVG Admin Server sends a list of valid
usernames/password hashes to AVG Admin Console. As the Admin Console is
controlled by the client, authentication can easily be bypassed.

Attackers can connect to the AVG Admin Server and manage clients just like a
legitimate administrator with full privileges using a modified version (checks
removed using binary patch) of AVG Admin Console.
```

Identification of Vulnerability → Vendor Notification → Vulnerability Validation and Resolution → Public Disclosure





Notification over a secure channel…

https://www.google.com/appserve/security-bugs/m2/new?rl=

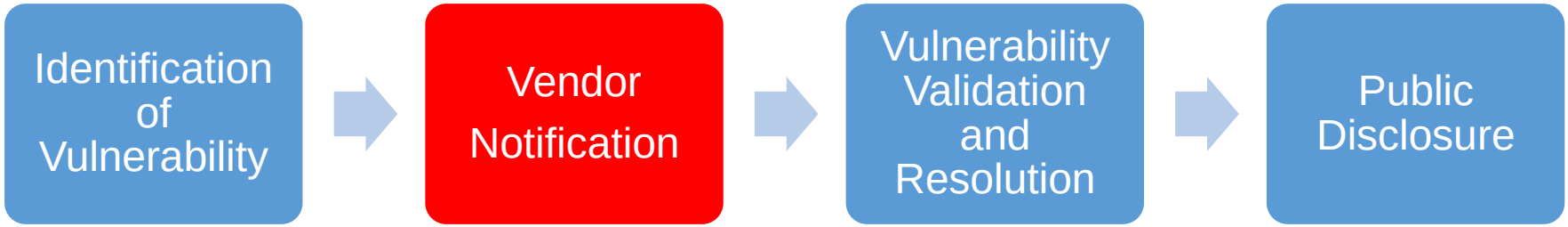
Google

Security Bug Report

Problem Description

Please describe the issue you wish to report

- I need assistance with my Google account.
- I want to remove content on Google Search, Youtube, or another service.
- I want to report a technical security bug in a Google product (SQLi, XSS, etc.).
- I want to report fraud, malware, or other problems not listed above.



Notification over a secure channel (not always easy)

Dear [redacted]

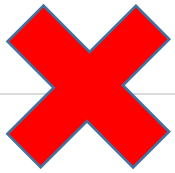
I've already sent you an email last week [redacted] without any reply.

A ticket [redacted] seems to have been created automatically and already closed as spam although it is not.

We have identified a critical vulnerability within your [redacted] software. I would need a security contact from your side to submit our security advisory.

If we don't receive a reply by tomorrow [redacted] we are going to publish the security advisory on [redacted] according to our responsible disclosure policy (attached at the last email).

best regards,



Identification of Vulnerability → Vendor Notification → **Vulnerability Validation and Resolution** → Public Disclosure

Vendor provides fix and publishes patch (fast!?)…

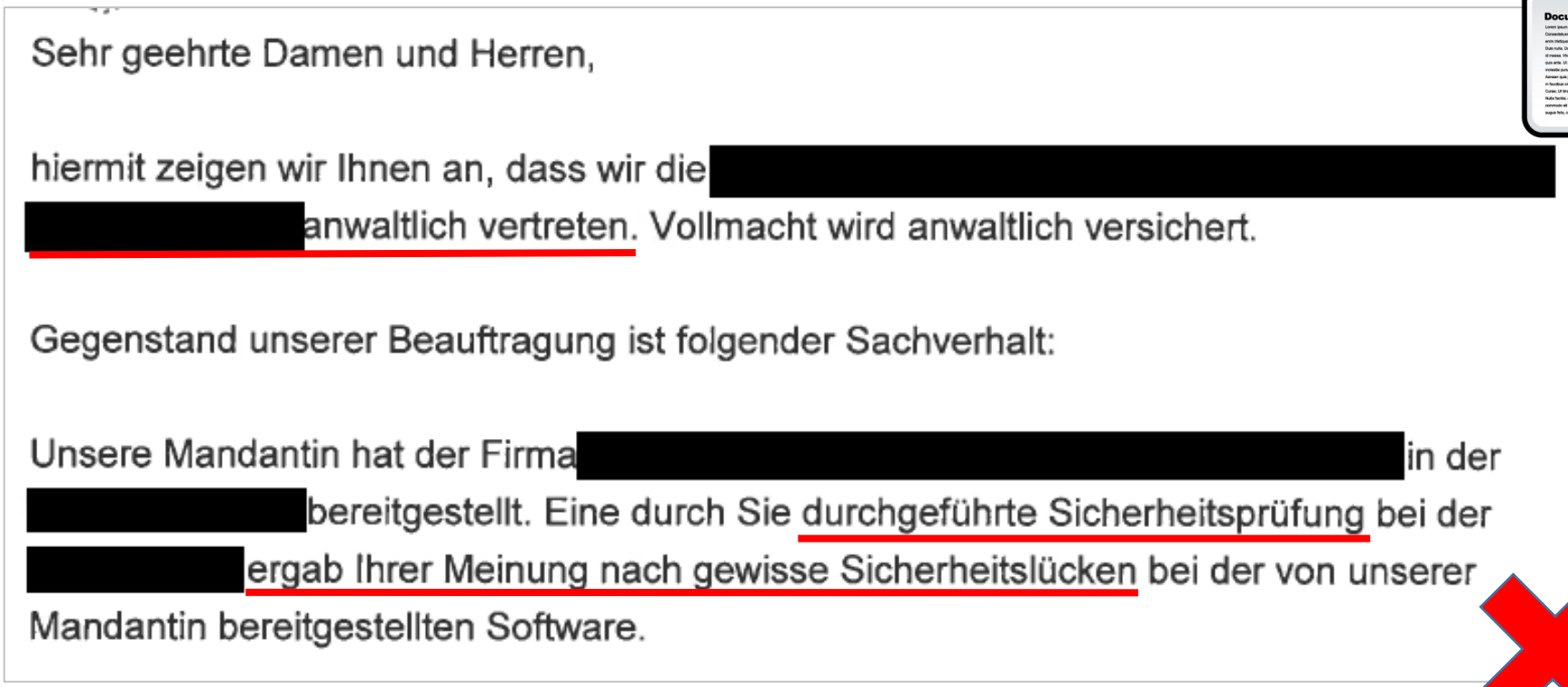
```
SEC Consult Vulnerability Lab Security Advisory < 201507
================================================================
2014-08-13: Contacting vendor through secalert_us@oracle.com
2014-08-14: Vendor response - vulnerbility will be investig
2014-08-15: Vendor response - issue will be tracked as S048
2014-08-22: Status update: Under investigation / Being fixed
2014-09-24: Status update: Issue fixed in main codeline, sche
2014-10-24: Status update: Issue fixed in main codeline, schedule
2014-11-24: Status update: Issue fixed in main codeline, scheduled for a f    CPU
2014-12-24: Status update: Issue fixed in main codeline, scheduled for a future CPU
2015-01-24: Status update: Issue fixed in main codeline, scheduled for a future CPU
2015-02-25: Status update: Issue fixed in main codeline, scheduled for a future CPU
2015-03-25: Status update: Issue fixed in main codeline, scheduled for a future CPU
2015-04-25: Status update: Issue fixed in main codeline, scheduled for a future CPU
2015-05-23: Status update: Issue fixed in main codeline, scheduled for a future CPU
2015-06-25: Status update: Issue fixed in main codeline, scheduled for a future CPU
2015-07-11: Issue is fixed in upcoming CPU, patches will be released on 2015-07-14
2015-07-16: Coordinated release of the security advisory
```

~ 1 Year Till Patch

Is this Responsible Disclosure?

Identification of Vulnerability → Vendor Notification → **Vulnerability Validation and Resolution** → Public Disclosure

Vendor provides fix and publishes patch (**or not**)…



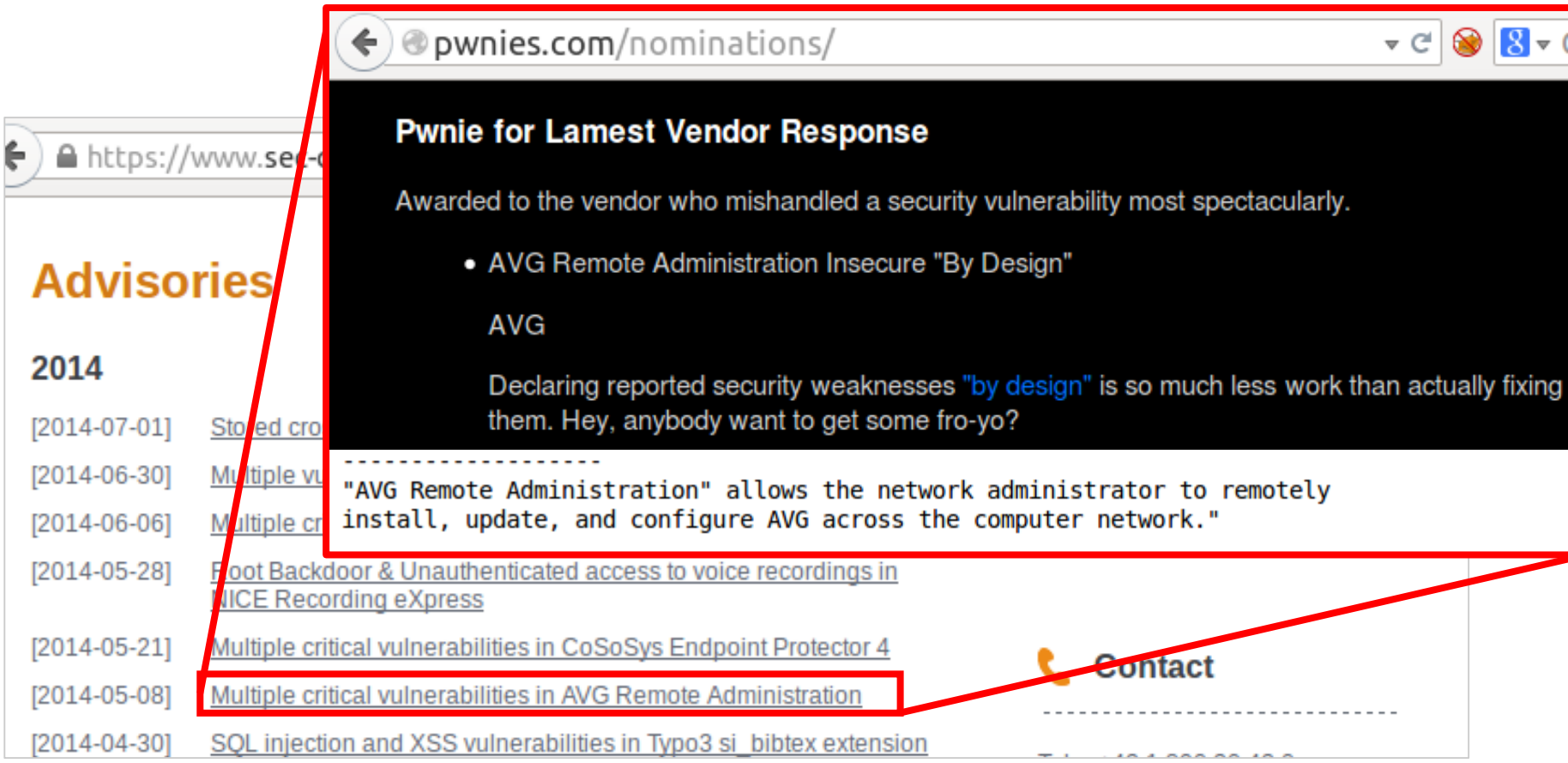
Sehr geehrte Damen und Herren,

hiermit zeigen wir Ihnen an, dass wir die [redacted] anwaltlich vertreten. Vollmacht wird anwaltlich versichert.

Gegenstand unserer Beauftragung ist folgender Sachverhalt:

Unsere Mandantin hat der Firma [redacted] in der [redacted] bereitgestellt. Eine durch Sie durchgeführte Sicherheitsprüfung bei der [redacted] ergab Ihrer Meinung nach gewisse Sicherheitslücken bei der von unserer Mandantin bereitgestellten Software.

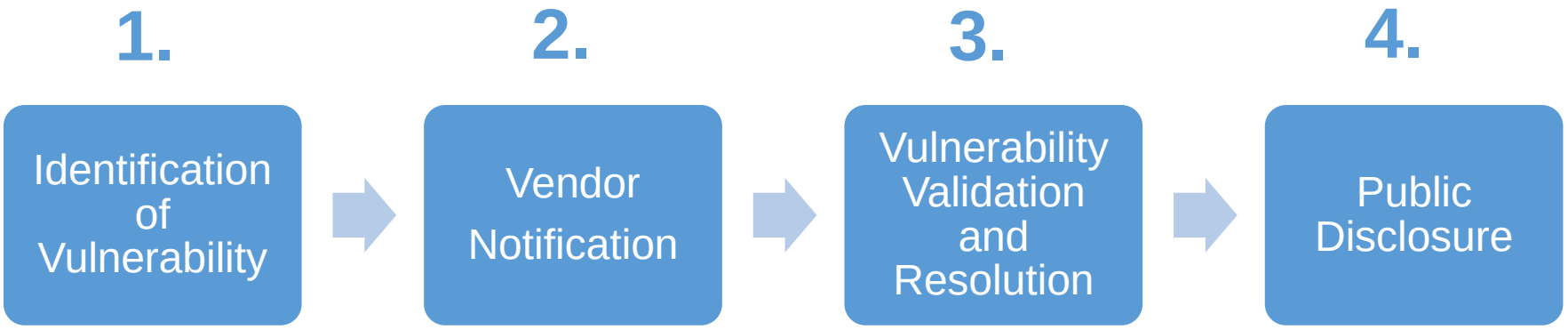
Identification of Vulnerability → Vendor Notification → Vulnerability Validation and Resolution → Public Disclosure



https://www.sec-consult.com/en/Vulnerability-Lab/Advisories.htm

Responsible Disclosure Done

Responsible Disclosure…



… is the „*rule of engagement*“ for a White Hat Hacker.

… a **fun process** with some interesting twists & turns.

… shows how **(in)**significant security is to certain vendors.

We want you!

SEC Consult

ADVISOR FOR YOUR INFORMATION SECURITY

- **Internship Junior Security Consultant**
- **Security Consultant**
- **White Hat Security Specialist**

career@sec-consult.com

Thank you!

Q && A