I’m Sorry to Inform You...

Dr. Marie Moe

Éireann Leverett

@MarieGGMoe

@blackswanburst
How we met...

I was a “young-ish” Mphil student

It was my first time disclosing 10K vulnerable systems

Neither of us had met...

...until FIRST MALTA

Funny story about that...

I was a “young-ish” incident responder

I was at a security meetup on my first week as duty officer
How did I come to trust him?

- Information sharing with NorCERT
- I read his thesis
- We met in person several times
- Responsive and professional contact
- Others vouched for him
# How did I come to trust her?

- Face to Face contact
- Willingness to use strong cryptography in emails
- She provided feedback (where others didn’t)
- Independent verification of facts
- Yearly communication
- Working further incidents

**Core question:**

- How do I know this info doesn’t flow straight to the offensive national team?
Information sharing

I inform DHS (How do I verify a “CERT”?)

DHS informs national CERTs

The CERTs investigates

NorCERT informs ISP

ISP informs its customers (vulnerable system owners)
In retrospect

I should have included vulnerabilities

- I was uncomfortable sending both IPs and vulnerabilities to one country for distribution
- So I just sent IPs to ICS-CERT
- That mean Marie couldn’t have much traction
- Since she didn’t have evidence of vulnerability
- The context was challenging to convey to the asset owners

In the future I’d give more details
Informing by proxy.

I used ICS-CERT/DHS in 2011

- They shared with 52 certs

I worked with 12 certs in 2012

- Codesys Vulnerabilities (detailed later)

Basic Process

- Send them an email about what you have
- Attach GPG key and sign email
- Offer them data
- When they respond, send it to them encrypted
How do you approach companies?

- **Find the Point of Contact**
  - Describe who you are
  - Allow them to verify you

- **Explain what you have**
  - Don’t speculate it’s impact on them
  - Clarify *precisely* the evidence you have

- **Let them think about the impacts**
  - Let them ask you questions until they’re satisfied
  - Encourage thoughtful, deliberate action, not quick or sudden responses
  - After-action: provide closure by revisiting

Let them think about the impacts
Who in the organisation should you be speaking to?

**Ideal:**
- Understands Technology
- Understands Security
- Has some level of responsibility for technology
- Previous Trust relationship established
- A CSO, CISO, or DFIR pro

**Not Ideal:**
- A service desk
- A CxO
- An engineer
- A PR person
- A lawyer
How do you explain vulnerabilities and exposure?

- **Global Scale and background**
  - How do they come in?
  - On the target list?
  - Found with exfiltrated credentials
  - Vulnerable systems found by external researcher

- **Tell the scope from your POV**
  - List of domains
  - List of IPs
  - List of CVEs
  - List of Services
  - Temporal information (between 7am and 10am)

- **Let them determine internal scope**
  - Assist with attack propagation knowledge
  - Assist with Technical Knowledge
  - Assist with knowledge of other victims

- **Revisit them when they’ve had time to investigate**
  - Now take notes on remediation
  - Invite them to share their success story in the future
One time during an incident: ‘assisted scope discovery’

Client thought only email had been compromised

I suggested it might be box that contained email

Client then thought single windows box was infected

Turned out to be wrong, but useful

Suggested looking at where profile had roamed

Forensics on a disk suggested exfiltration of data

Knowledge of IODINE allowed me to suggest DNS traffic examination in openflow

Got a handle on volume of exfiltrated data
How do you tell them they’re owned/infected?

- Global scope
  - How do they fit in
  - Targeted?
  - Compromised?
  - Observed traffic in sensors or sinkholes?

- Indicators of compromise
  - Exactly what to look for in logs and systems
  - Exact timestamps and timezones
  - IDPS signatures could be helpful

- Leaked credentials should be sanitized
  - Include enough context info to get their attention

- Use secure channels for sharing the more sensitive stuff

- Follow-up may be required/expected
How do you tell them they’re causing someone else harm?

<table>
<thead>
<tr>
<th>Watering holes</th>
<th>Malvertising</th>
<th>DDoS Reflectors</th>
<th>Botnets</th>
<th>Spam</th>
</tr>
</thead>
<tbody>
<tr>
<td>URLs and IPs Timestamps</td>
<td>URLs and IPs Timestamps</td>
<td>Traffic captures</td>
<td>IPs</td>
<td>Domain</td>
</tr>
<tr>
<td>Sample exploit and CVEs</td>
<td>Sample malverts</td>
<td>Log files</td>
<td>Indicators of Compromise</td>
<td>IP ranges</td>
</tr>
</tbody>
</table>
The CodeSys Story

1. Ten Autonomous Systems containing the largest number of vulnerable PLCs

<table>
<thead>
<tr>
<th>PLCs Found</th>
<th>ASN</th>
<th>CC Registrar</th>
<th>AS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>6327</td>
<td>CA</td>
<td>arin Shaw Communications Inc.</td>
</tr>
<tr>
<td>9</td>
<td>6830</td>
<td>AT</td>
<td>ripencc Liberty Global Operations B.V.</td>
</tr>
<tr>
<td>12</td>
<td>5610</td>
<td>CZ</td>
<td>ripencc Telefonica Czech Republic, a.s.</td>
</tr>
<tr>
<td>21</td>
<td>28929</td>
<td>IT</td>
<td>ripencc ASDASD-AS ASDASD srl</td>
</tr>
<tr>
<td>25</td>
<td>12605</td>
<td>AT</td>
<td>ripencc LIWEST Kabelmedien GmbH</td>
</tr>
<tr>
<td>28</td>
<td>3269</td>
<td>IT</td>
<td>ripencc Telecom Italia S.p.a.</td>
</tr>
<tr>
<td>28</td>
<td>3303</td>
<td>CH</td>
<td>ripencc Swisscom (Switzerland) Ltd</td>
</tr>
<tr>
<td>43</td>
<td>1136</td>
<td>EU</td>
<td>ripencc KPN Internet Solutions²</td>
</tr>
<tr>
<td>43</td>
<td>286</td>
<td>EU</td>
<td>ripencc KPN Internet Backbone</td>
</tr>
<tr>
<td>44</td>
<td>3320</td>
<td>DE</td>
<td>ripencc Deutsche Telekom AG</td>
</tr>
</tbody>
</table>

Table 2. Ten Countries containing the largest number of vulnerable PLCs

<table>
<thead>
<tr>
<th>PLCs Found</th>
<th>Country</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>CA</td>
<td>CA</td>
</tr>
<tr>
<td>21</td>
<td>ES</td>
<td>ES</td>
</tr>
<tr>
<td>29</td>
<td>CZ</td>
<td>CZ</td>
</tr>
<tr>
<td>33</td>
<td>AT</td>
<td>AT</td>
</tr>
<tr>
<td>33</td>
<td>US</td>
<td>US</td>
</tr>
<tr>
<td>38</td>
<td>CH</td>
<td>CH</td>
</tr>
<tr>
<td>60</td>
<td>PL</td>
<td>PL</td>
</tr>
<tr>
<td>64</td>
<td>NL</td>
<td>NL</td>
</tr>
<tr>
<td>80</td>
<td>DE</td>
<td>DE</td>
</tr>
<tr>
<td>81</td>
<td>IT</td>
<td>IT</td>
</tr>
</tbody>
</table>
How not to do it.

- In an embarrassing or challenging way
- Without support or feedback
- Without follow up contact
- In public
- Without actionable information
- On film
- Victim blaming
- Without legal consideration
The shock effect 1

Source: https://youtu.be/okhfDkmAoY?t=218
The Null CTRL article series

Journalists warned system owners and Norwegian NSA of 2500 critical data flaws

How two journalists set out on a mission to test the data security in the whole of Norway.

Source: http://www.dagbladet.no/2014/01/06/nyheter/nullctrl/shodan/english/english_versions/30861347/
The shock effect 2

Source: http://www.dagbladet.no/2013/10/14/nyheter/innenriks/nullctrl/datasikkerhet/29071043/
Havex/Dragonfly/Energetic Bear

August 28, 2014

Hundreds of Norwegian energy companies hit by cyber-attacks

Share this article: Facebook Twitter LinkedIn Google+

Approximately 300 oil and energy companies in Norway have been hit by one of the biggest cyber-attacks ever to have happened in the country, a government official is reported to have claimed.

As first reported by The Local and Dagens Næringsliv, the National Security Authority Norway (Nasjonal Sikkerhetsmyndighet – NSM) detailed how 50 companies in the oil sector were hacked and how another 250 have been warned that they may have been hit too.

NSM is Norway's prevention unit for serious cyber-attacks and, like CERT-UK in Great Britain, warns companies about the newest threats. It took part of the CyberEurope2014 exercise in June.

The companies themselves haven't been named – although NSM is investigating whether the computer systems at Statoil, Norway’s largest oil company, were targeted. Technical details are also few and far between at this moment in time.

Subject: Shipping notification

Your parcel has arrived at May 27th, 2014. Courier was unable to deliver the parcel to you.

Get your label and show it in the nearest post office to get a parcel.

[Link]

Print Shipping Label

Copyright 2014 Posten Norge. All Rights Reserved.
Dear Colleagues,
You are invited to participate in the forthcoming International Conference on Energy and Environment Research (ICEER 2014), which will be held in Madrid, Spain during July 18-19, 2014. ICEER is an event that focuses on the state of the art technologies pertaining to Energy and Environment Research. The applications of Energy and Environment Research to such domains as astronomy, biology, education, geosciences, security and health care are among topics of relevance to ICEER. It is a technical congregation where the latest theoretical and technological advances on Energy and Environment Research are presented and discussed. We expect that the conference and its publications will be a trigger for further related research and technology improvements in this important subject. ICEER promotes fundamental and applied research continuing advanced academic education and transfers knowledge between involved both sides of and the Energy and Environment Research.

For registration information you are to contact the conference Registrar.

Please share this information with your colleagues.

Sincerely

International Conference on Energy and Environment Research Committee.
mbCHECK (EUROPE)

- Diagnostic program mbCHECK for mbCONNECT24 server location EUROPE
- Version: V 1.1.2
- MD5 Checksum: A61FC8F09F99E57B10F663923ECD472

mbCHECK (USA/CAN)

- Diagnostic program mbCHECK for mbCONNECT24 server location USA / CAN
- Version: V 1.1.2
- MD5 Checksum: BB977F03FEF48CE28DA48199EE8CFD6F
In retrospect

Sending out physical letters was not very useful

The crisis management personnel were not always the best contact points

The media “got it wrong”, however the effect was good nonetheless

With the KraftCERT establishment we should do better the next time
Good Reactions

I accept the risk

Here’s some more info on that attacker

Thank you

Thank you, we’ll pass this to the DFIR team

That’s a larger scope than we realised

It’s a honeypot/Lab/testsystem
Bad Reactions

I’ll sue you

We unplugged it and reinstalled the OS

You’re interfering in private business

It’s all hype

We are not liable for that

We followed the standards

A third party configured that
Conclusion

- Introduce yourself
- Give background
- Give specifics
- Have a good bedside manner
- Assist scope discovery
- Return later
- Make them a success story
Questions
Thank you

marie.moe@sintef.no
eireann.leverett@cantab.net