Cyber Attacks and Digital Forensics on Industrial Systems

Daniel Lewis

daniel.lewis@southwales.ac.uk
Senior Research Fellow
University of South Wales

daniel@awencollective.com
Entrepreneur/Cofounder/CEO
Awen Collective

University of South Wales
Prifysgol De Cymru

Awen collective

Attacks on Industrial Control Systems

- Stuxnet – 2010
  - Caused damage
  - Iran - 14 sites, inc. a nuclear-enrichment plant
  - Chevron in California
- Duqu – 2011
  - Iran – made to steal information of ICS devices and networks
- Flame – 2012
  - Undetected pre-cursor to Stuxnet
  - Used for cyber-espionage
- Gauss – 2012
  - Used for cyber-surveillance

University of South Wales
Prifysgol De Cymru

Awen collective

Attacks on Industrial Control Systems

- Ukrainian Power Grid - Hacked
  - Switched off by hackers – Dec 2015 & Dec 2016
- Turkish Oil Line - Hacked
  - 2008 Hacking of alarms & communications causing a spill of 30k barrels of oil
- Turkish Electricity Distributor – Hacked
  - Deleted bills worth 1.5 trillion Turkish Lira in 2014
- German Steel Mill – Hacked
  - 2014 spear phishing email attack, led to blast furnace explosion
- "Kemuri" Water Company – Hacked
  - Hackers changed chemical levels in tap water in 2016
- Pharma – Dragonfly Hacked
  - Planted in 2010, not discovered until 2013. Stole info, particularly IP from manufacturers.

University of South Wales
Prifysgol De Cymru

… and many more…

…… Known & Unknown

Awen collective

Prevention : Cyber Defence

- Patch & Update Management
- Employee Background Checks
- Cyber security essentials:
  - Firewalls,
  - A.V.,
  - User Access Control
- Employee education
  - USB Attacks
  - Email Phishing
  - Plug & Play Devices
- Anomaly Detection Systems
  - e.g. Nozomi, CyberX, Indegy
- Incident Response Plan
  - Forensics Readiness Plan

University of South Wales
Prifysgol De Cymru

Awen collective

Investigation : Digital Forensics

- An attack happens on an ICS
  - Begin Investigating: Internal/External Incident Response Team
  - Notify: National Cyber Security Centre (NCSC)
  - Begin Investigating: Police, with help from NCSC & relevant gov. departments
  - If state-sponsored attack: Military get involved

- Very important to have a Forensics-Readiness Plan in place
  - To reduce operations downtime
  - To speed up the digital forensics analysis

- Awen Collective is a spin-out company of the USW to help with digital forensics in industrial environments.

University of South Wales
Prifysgol De Cymru

Awen collective

Cyber Attacks and Digital Forensics on Industrial Systems

Daniel Lewis

daniel.lewis@southwales.ac.uk
Senior Research Fellow
University of South Wales

daniel@awencollective.com
Entrepreneur/Cofounder/CEO
Awen Collective

University of South Wales
Prifysgol De Cymru

Awen collective