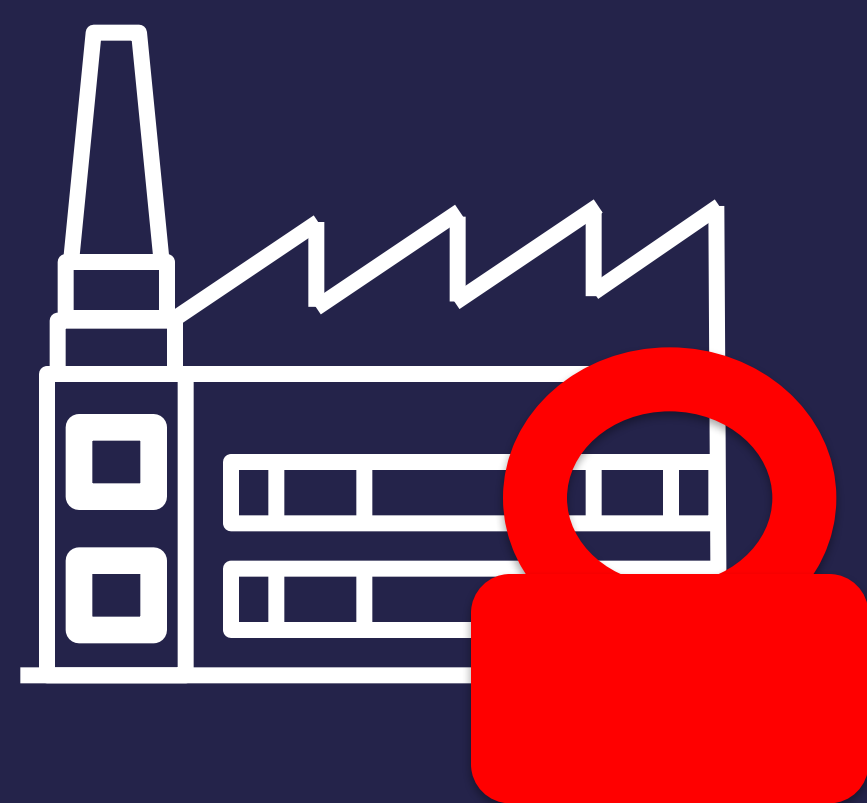


The Threat of Ransomware in Energy Delivery Systems

David M. Nicol, Franklin W. Woeltge Professor of Electrical and Computer Engineering | University of Illinois at Urbana-Champaign

The Threat



To: chief.executive.officer@gotham.city.power.com
From: chief.security.officer@gotham.city.power.com

Mr CEO---this message is not authored by your CSO. We are the Citizen's Alliance for Clean Energy, and we have control of your cyber systems, in particular, of your Moon River power plant. Ask your engineers, they've lost control of the plant.

Our software will cause destruction of its generators by midnight tonight, unless you publically announce the plant's immediate retirement. On seeing this announcement we will tell you how you can disable that timer. Be aware however that any subsequent actions not directly connected to a shutdown will trigger the destruction.

Happy Halloween!
Citizen's Alliance for Clean Energy

Actual Events

The Register
Security
Michigan electricity utility downed by ransomware attack
Don't click on the links, do ...
By Richard Chirgwin 3 May 2016 at 01:40

ET CIS
Home News Whitepapers CISO Mind Speak CISO Wall Interviews CISO TV Brand Solutions
IT Security News / Latest IT Security News / Incident Response
Incident Response West Bengal WBSECL wannacry Ransomware Power distribution Malware incident response
Ransomware WannaCry hits Bengal power utility
The utility is now running the risk of witnessing larger numbers of PCs getting affected as this ransomware can infect other PCs in a network and could reach into servers unless it has patched a vulnerability that this virus uses to hack computers.
Debjoy Sengupta | ET Bureau | May 15, 2017, 17:52 IST

But only Internet-facing business functions were disabled

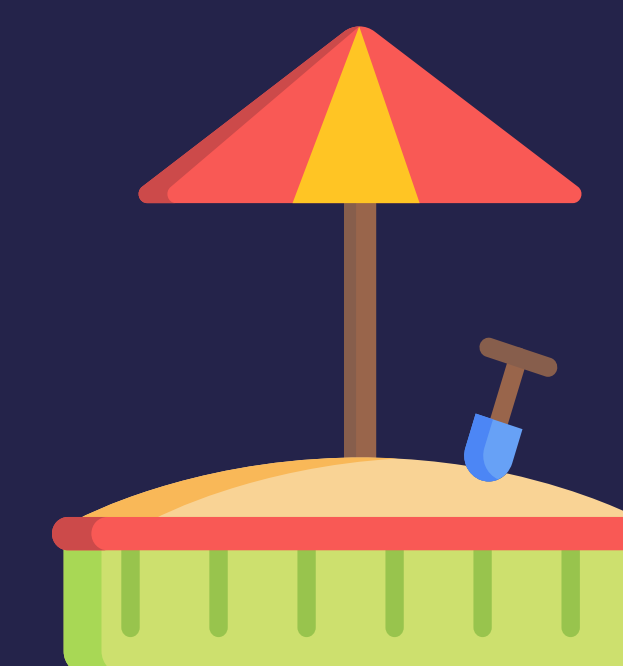
Solutions



Better computer hygiene



Training

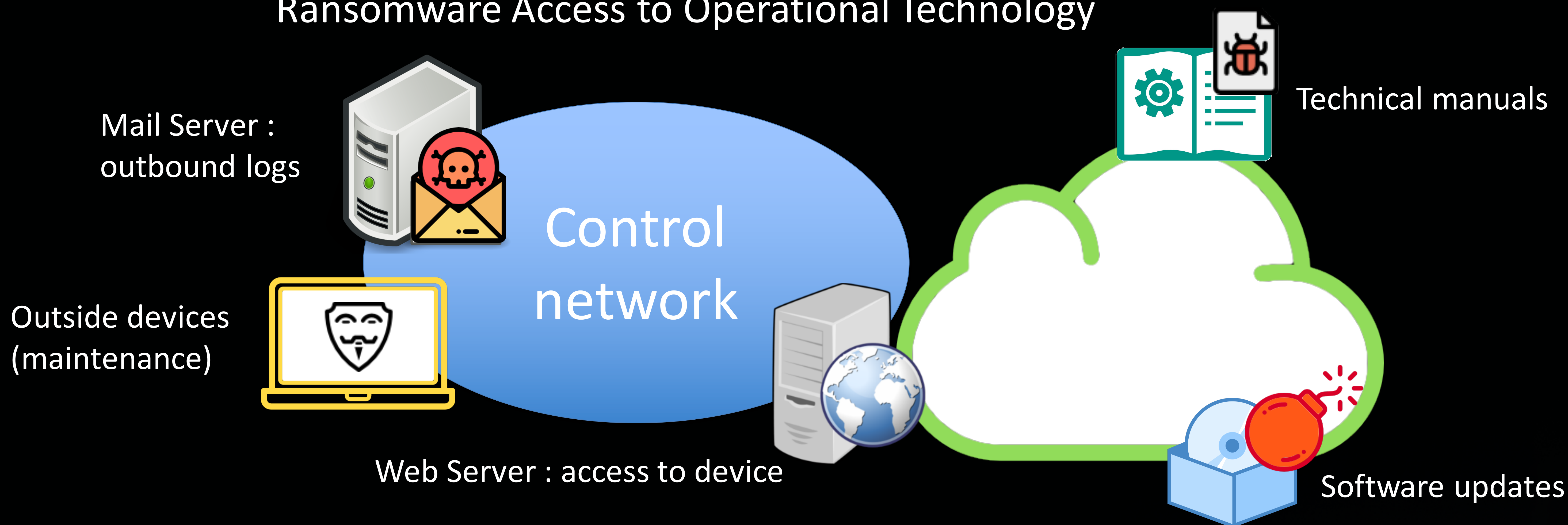


Sandboxing



White listing

Ransomware Access to Operational Technology



Additional Prevention



Strict controls



Multifactor authentication

Mitigation



Virtualized ICS networks & devices



SPECIAL CYBER OPERATIONS
RESEARCH AND ENGINEERING



Computational Cybersecurity in Compromised Environments
2017 Fall Workshop | October 23-25, 2017 | Atlanta, Georgia