Thoughts on ISP security

Kauto Huopio
FICORA / NCSC-FI

My two cents

- Take this very carefully:
  (FICORA 67 A / 2015 M)

Section 8 Management network and management connection traffic

The telecommunications operator must appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to be made to the communications network or service components.

Why?

- A number of cases where attackers with significant resources have been **accessing core network infrastructure, modifying core/edge router configurations, even patching router OS in order to gain access to specific customer traffic**

Why?

TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles

bics
a belgacom company

Why?

The Telegraph

HOME | NEWS | SPORT | BUSINESS | ALL SECTIONS

Technology Intelligence

Gadgets | Innovation | Big Tech | Start-ups | Politics of Tech | Gaming | Podcast | Tech Jobs | Newsletter

Technology Intelligence

Hackers targeting UK energy grid, GCHQ warns

share

MORE STORIES

1 Even as a Remainer, I can see that the politically compromised Brexit we are heading for is...

2 Theresa May accused of 'sneaky' betrayal over Brexit vote as deal with Tory rebels collapses

3 Theresa May poised to give NHS £4bn-a-year boost funded by Brexit dividend, borrowing and income tax

4 The SNP return to the Commons... for yet another orgy of self-pity

5 EU fights to avoid post-Brexit security talks split

Why?

Irish power grid compromised by foreign actor: report

BY JOE UCHILL - 08/08/17 10:07 PM EDT

75 SHARES

Why?

A foreign power compromised the cybersecurity of the state-owned Irish power grid company EirGrid, Ireland's Independent newspaper reports.

The report, issued Monday in Ireland, says that the telecommunications company Vodafone discovered last month that hackers had compromised its systems more than two months prior.

The attackers then installed eavesdropping software on the routers used by EirGrid and were able to see encrypted communications sent by the company.

Recommendations

- From network engineer workstations – access internet from a terminated Citrix session (Yes. I know this will cause serious pain.)
- Remote access to admin segments only with strong authentication
- Logging of all access to admin networks
- Logging of all access to network elements
- Logging of all commands sent to network elements
- Storage of logs in a separate log storage network with no access from regular admin networks
- Detection of lack of logs from network elements
- Network element running OS image verification

Also remember this:

Section 10 Closure of unnecessary services and protocols

The telecommunications operator must ensure that no services or protocols that are unnecessary for the provided communications service are enabled in the components or the associated ports of communications networks or services in the operator's interconnection or customer interfaces.

Reading FICORA 67 A / 2015 M with attached explanatory notes with a thought highly recommended

Any recommendations for improvement welcome ☺

Viestintävirasto

Finnish Communications Regulatory Authority

www.ficora.fi