HOW NOT TO INTEGRATE A CPE

PASCAL GLOOR @ SWINOG-35

DISCLAIMER OR DISC LAMER…

THIS IS NOT A SERIOUS TALK*

*ALL CHARACTERS (OR DEVICES) APPEARING IN THIS TALK ARE FICTITIOUS.

ANY RESEMBLANCE TO REAL PERSONS (OR DEVICES), LIVING OR DEAD, IS PURELY COINCIDENTAL

THIS IS NOT A SERIOUS TALK**

**LEAVING THE ROOM IS POSSIBLE, IN THEORY

SCOPE

SCOPE

CONSUMER ACCESS CPE

CONSUMER

CONSUMER

ACCESS

FIBER…

ACCESS

{XDSL, DOCSIS, FTTH} AKA FIBER

FRENCH: JIG OR DIJIG
GERMAN: GIGABIT OR ZÄGIG

(SPEEDS BETWEEN NOTHING AND A LOT)

CPE

CONSUMER CPE I SAID!@!!!

CPE

TYPICAL CONSUMER SETUP

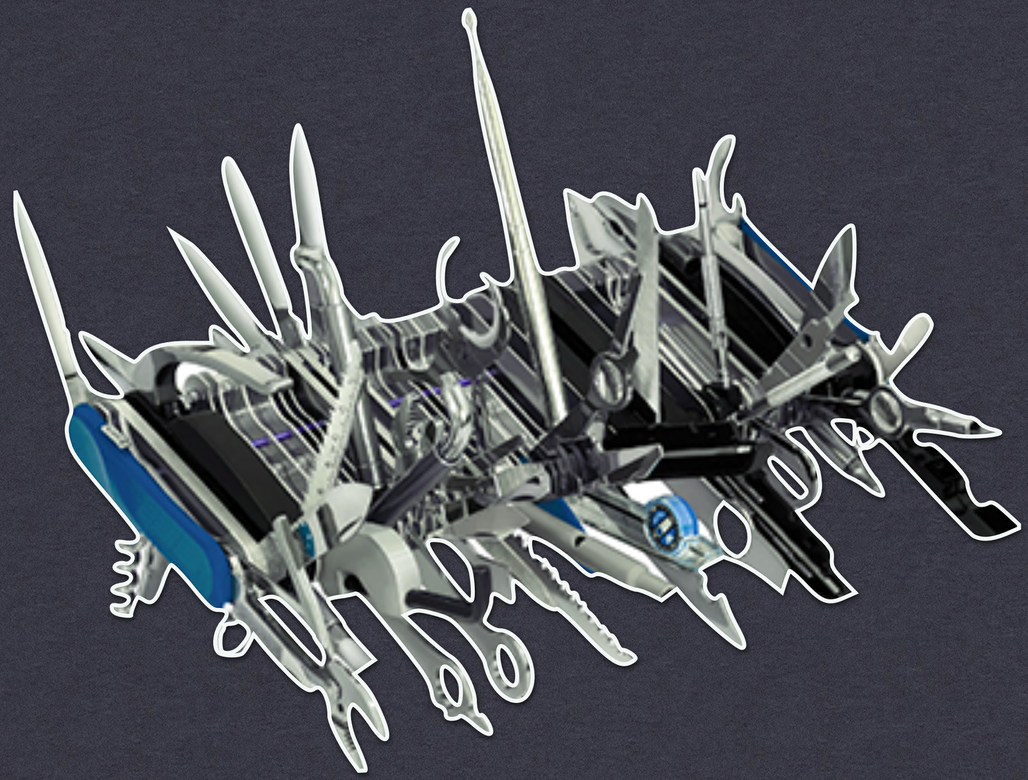
ACQUISITION

SELECTING A VENDOR / DISTRIBUTOR

GO FOR THE COOL SALESMAN, SHADY IF POSSIBLE AND CHEAPEST POSSIBLE CPE

DEVICE FEATURES

CPE MUST HAVE AT LEAST 200 FEATURES.



TESTING

DOES IT TURN ON?
DOES IT BLINK?
CAN YOU SURF ON THE TOILET OVER WEEELAHN (GERMAN) OR WIFIT (FRENCH)?

INTEGRATION

INTEGRATION

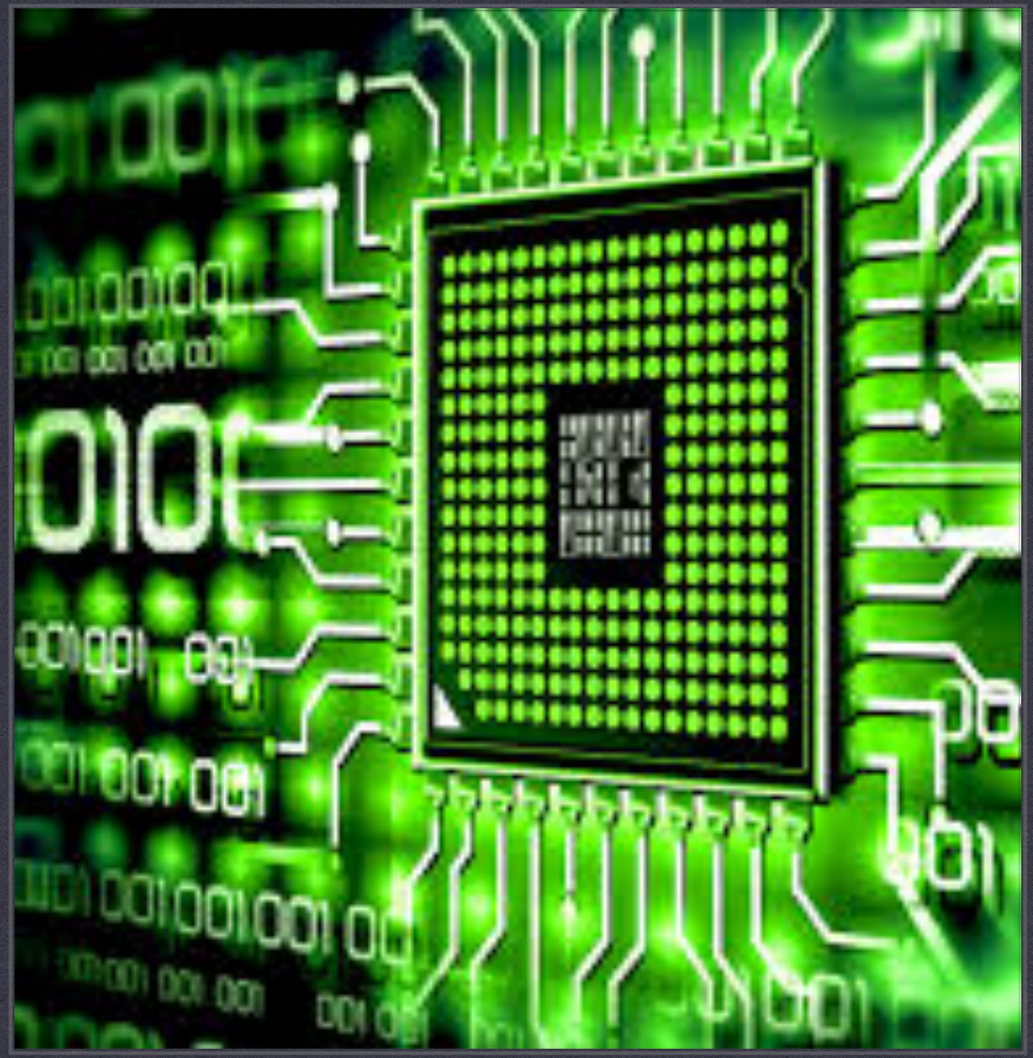
PROS:

- DON’T NEED TO CARE
- DON’T NEED TO LEARN ANYTHING
- DON’T NEED TO SUPPORT IT

CONS:

UPGRADES

- IGNORE THEM
- BUY A NEW CPE (REWIND THE SLIDES TO UNDERSTAND HOW TO)



LUCKY?

FREE ADVERTISING !!!

Deutsche Telekom warns cyber attack hit up to 900,000 customers

German telecoms group investigates whether hackers caused network outages

Among the trade-offs is the danger of computers increasing the risk of “flash crashes” and exposure to hackers © Reuters


WARNING


DANGER -
NO GO AREA


WARNING


DANGER -
NO GO AREA

THE NEXT SLIDE MIGHT BE SERIOUS!

How to integrate a CPE seriously, seriously!

How to integrate a CPE seriously, seriously!

* Select **distributor** on its ability to **support you**

How to integrate a CPE seriously, seriously!

* Select **distributor** on its ability to **support you**
* Select **CPE** on its proven (tested!!!) **capabilities** and **interoperability**

How to integrate a CPE seriously, seriously!

* Select **distributor** on its ability to **support you**
* Select **CPE** on its proven (tested!!!) **capabilities** and **interoperability**
* Integrate and test with the help an **experienced partner**, but keep the knowledge in-house!

How to integrate a CPE seriously, seriously!

* Select **distributor** on its ability to **support you**
* Select **CPE** on its proven (tested!!!) **capabilities** and **interoperability**
* Integrate and test with the help an **experienced partner**, but keep the knowledge in-house!
* **Upgrade firmware** regularly (check the new firmware can upgrade/downgrade)

How to integrate a CPE seriously, seriously!

* Select **distributor** on its ability to **support you**
* Select **CPE** on its proven (tested!!!) **capabilities** and **interoperability**
* Integrate and test with the help an **experienced partner**, but keep the knowledge in-house!
* **Upgrade firmware** regularly (check the new firmware can upgrade/downgrade)
* **Scan** your **CPE,** positive/negative testing and defaults are a bitch!!!

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB
Melde- und Analysestelle Informationssicherung MELANI

INFORMATIONSSICHERUNG

LAGE IN DER SCHWEIZ UND INTERNATIONAL

Halbjahresbericht 2018/II (Juli – Dezember)

4.3.1 Quickline-Modems für SNMP-Amplification Attacken missbraucht

Wie der Internetanbieter «Quickline» am 11. Oktober 2018 in einer Medienmitteilung publizierte, hatte der Provider während zweier Wochen mit unregelmässigen Störungen zu kämpfen. Beeinträchtig von der Störung waren sowohl die Dienste Fernsehen, Internet und Telefonie, wobei das Problem nicht bei allen Kunden gleich und auch nicht in gleichem Ausmass auftrat. Als Ursache konnte eine Schwachstelle bei einem Modem-Typ identifiziert werden. Analysen ergaben, dass die Kunden nicht direkt im Visier der Angreifer standen. Sie dienten nur als Mittel zum Zweck, um einen Angriff gegen Dritte durchzuführen. Es handelte sich um einen sogenannten «SNMP-Amplification» Angriff. Dabei wird das Simple Network Management der Geräte verwendet, um eine Anfrage zu verstärken und diese schlussendlich auf das Ziel zu lenken, um dieses zu überlasten. Die Modems werden zu diesem Zweck nicht infiziert,

[11] https://www.computerworld.ch/security/hacking/smart-home-in-minuten-hacker-da-1435426.html (Stand: 31. Januar 2019)
[12] https://iotsecuritymapping.uk/ (Stand: 31. Januar 2019)

sondern der Angreifer nutzt lediglich den Umstand, dass das SNMP System gegen aussen offen verfügbar ist. Die Störungen bei den Kunden sind aufgetreten, weil die Anfragen unabsichtlich auch die Modems überlastet und somit Instabilitäten hervorgerufen haben dürften. Da nicht alle Quickline-Kunden den gleichen Modem-Typen benutzen, waren nur 5% oder rund 9000 Kunden betroffen. Wie lange die Modems anfällig auf die SNMP-Amplification Angriffe waren, ist nicht bekannt. Um die Schwachstelle zu beheben, hat Quickline mehrere Massnahmen ergriffen. Dabei handelte es sich vor allem um Filter im Netz und ein zusätzliches Absichern der betroffenen Modems. Quickline hat rechtliche Schritte eingeleitet.

HALF-YEAR MELANI REPORT 2018/II (SWISS INTELLIGENCE)

How to integrate a CPE seriously, seriously!

* Select **distributor** on its ability to **support you**
* Select **CPE** on its proven (tested!!!) **capabilities** and **interoperability**
* Integrate and test with the help an **experienced partner**, but keep the knowledge in-house!
* **Upgrade firmware** regularly (check the new firmware can upgrade/downgrade)
* **Scan** your **CPE,** positive/negative testing and defaults are a bitch!!!
* Maintain a good and **healthy relationship** with your vendor, distributor and integration/testing partner, you will need them again, it's **not a one time thing**!


QUESTIONS?
THANK YOU
SEE YOU @BEER
FOLLOW ME (OR NOT)
@SPALE75