Fachhochschule Münster University of Applied Sciences

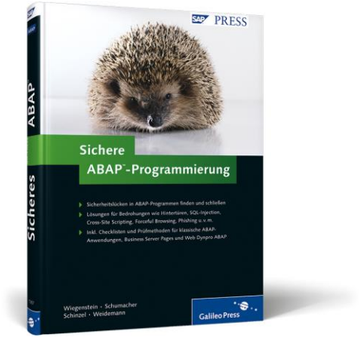
Scannen des gesamten IPv4 WWW

Prof. Dr.-Ing. Sebastian Schinzel

Email: schinzel@fh-muenster.de
Web: https://www.its.fh-muenster.de/
Twitter: @seecurity

Sebastian Schinzel

- 2013 berufen als Professor für IT-Sicherheit
- Leitet Gruppe des Labor für IT-Sicherheit

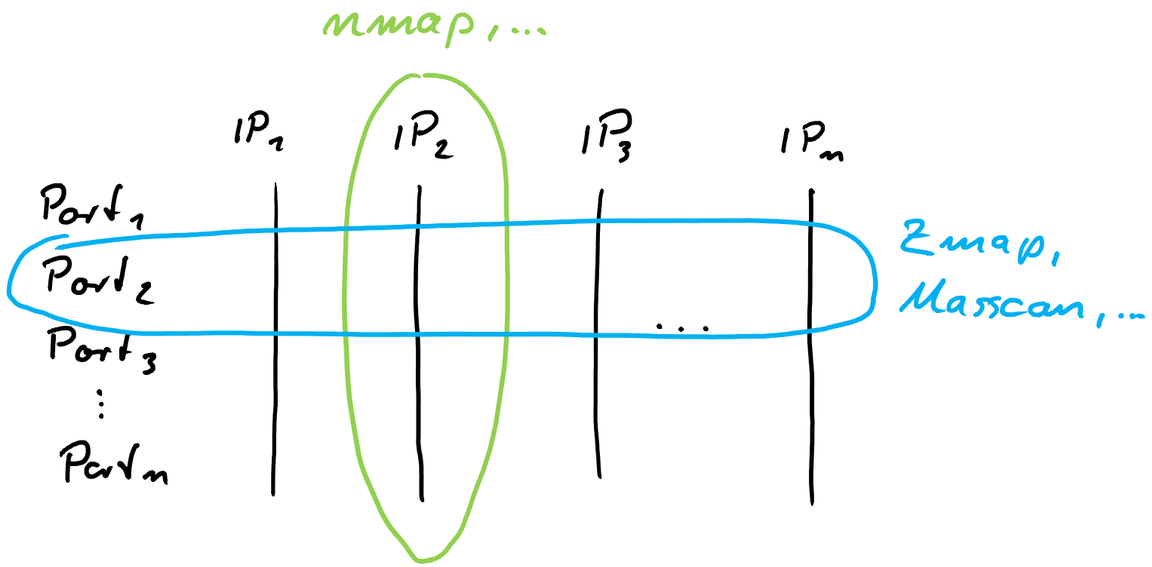


Forschungsthemen:

- Offensive IT-Sicherheit (Penetrationstests, Angriffstechniken, Schwachstellenanalysen)
- Sichere Softwareentwicklung

Portscanning heute

- nmap
  - ist ein Standardwerkzeug in der Reconnaissance-Phase von Penetrationstests
  - ist nicht optimiert für das Scanning vieler Systeme
- Vertikales Scanning: Prüfe viele Ports auf wenigen Systemen
- Horizontales Scanning: Prüfe wenige Ports auf vielen (allen) Systemen



Shodan

Sie suchen anfällige Systeme im Internet?

- Shodan: Suchmaschine speziell für das Auffinden (anfälliger) Internetdienste
- „Shodan Hacking Database“ enthält mehr als 100 Suchstrings anfälliger Systeme im Internet
- Voller Zugriff auf Suchergebnisse nur für zahlende Kunden
- Datenerhebungsmethodik unklar

Internet Census 2012

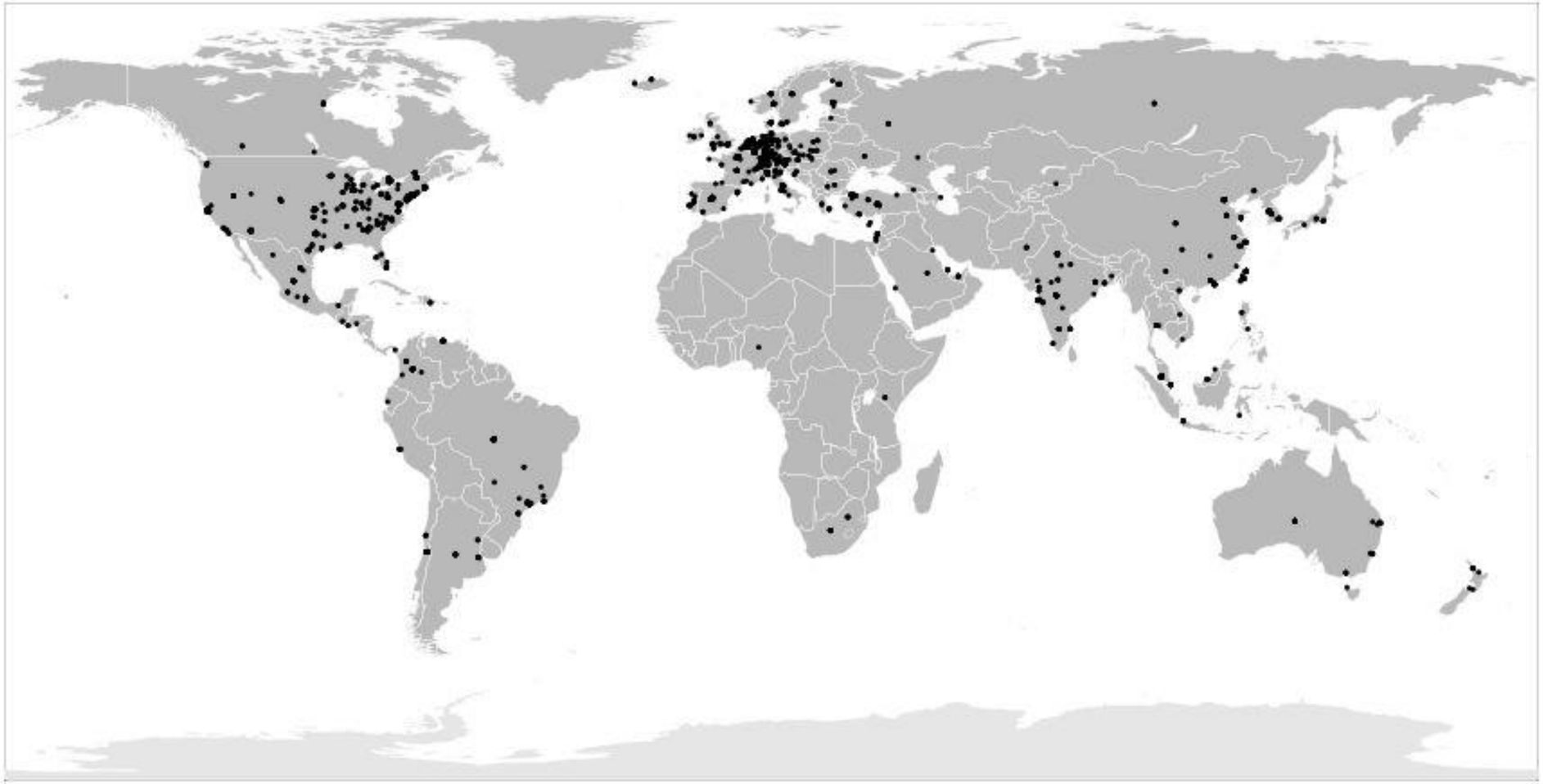
Sie suchen anfällige Systeme im Internet?

- Internet Census 2012 Datenbank
  - Eine Hacker-Gruppe kompromittierte Tausende von Routern im Internet und scannte von ihnen aus das gesamte Internet
  - 8 Terabyte große Datenbank mit Scanresultaten
- Beispiel:
  9895 offene Netzwerkports mit SAP-Systemen
- Für Details siehe: Schinzel/Thünemann/Löhr: *„Internetzensus - Das Internet scannen und auf Schwachstellen untersuchen “.* Heise Verlag, iX Security Special 09/2014

Internet Census 2012

SAP-Webserver auf Port 80

3106 Instanzen



Portscanning heute

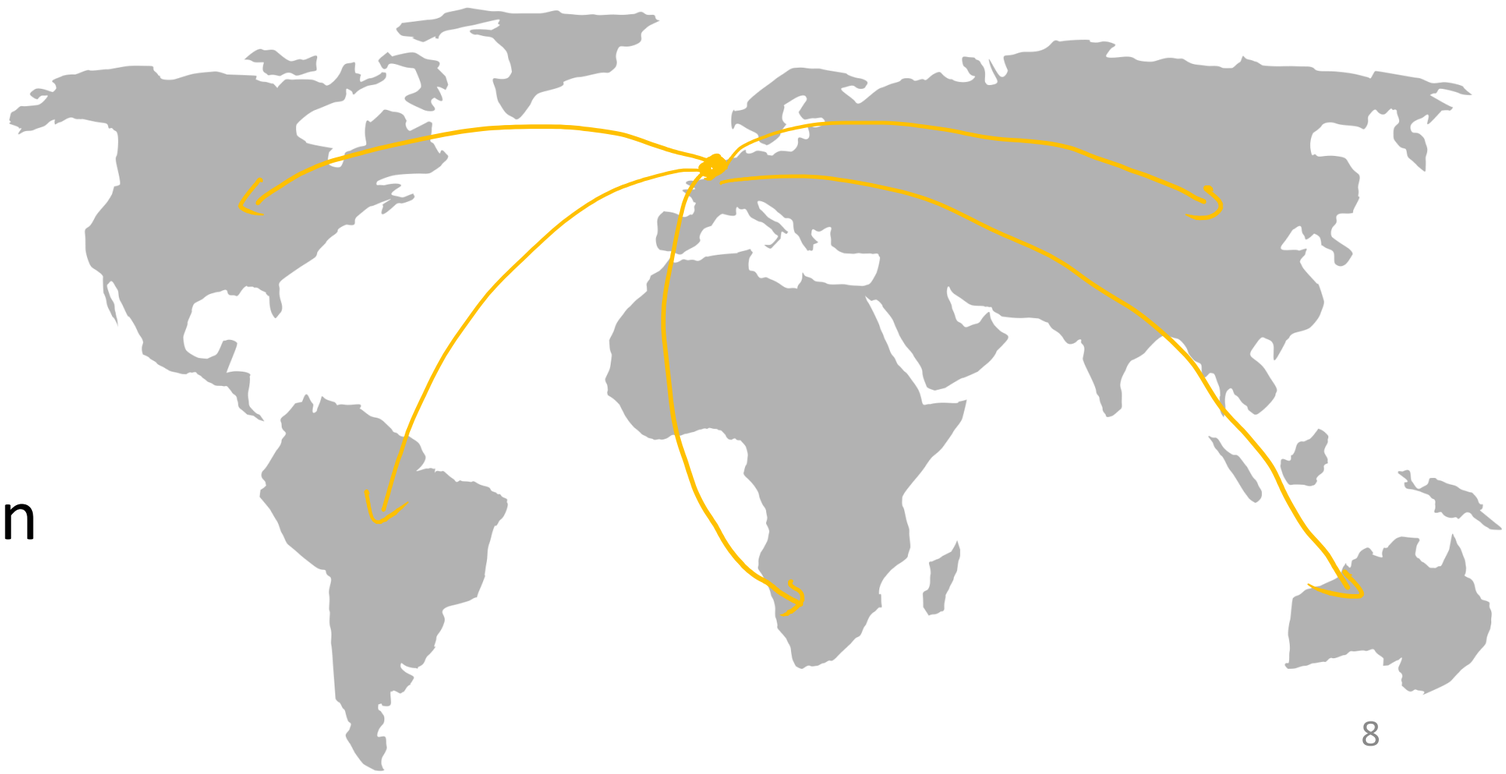
Horizontale Scanner

- Zmap: University of Michigan https://zmap.io/
  - Trennt Senden und Empfangen von Threads
  - Kodiert Zustand in den gesendeten Paketen
  - Pseudozufällige Scanreihenfolge der IPs
  - Saturiert 1 Gbit/s (scannt 0.0.0.0/0 in ~40 Minuten)
- Masscan: Rob Graham https://github.com/robertdavidgraham/masscan
  - Lagert Funktionalität in Kernel aus
  - Saturiert 10 Gbit/s (scannt 0.0.0.0/0 in ~3 Minuten)

Projekt Zensus

Projekt Zensus

- Durchführung eigener Internet-Scans aus IT-Sicherheit Labor heraus
- Scanning-Infrastruktur im Labor wird aktuell massiv ausgebaut*
- Ziel: reguläre Scans des gesamten IPv4-Adress-bereichs um belastbare Zahlen über die Verteilung anfälliger Systeme zu finden
- Herausforderung: IPv6



*Gefördert durch BMBF „FH BASIS“

Forschung (Beispiel)

Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices
Nadia Heninger, Zakir Durumeric, Eric Wustrow, J. Alex Halderman
Proceedings of the 21st USENIX Security Symposium, August 2012.

Warum Scanning?

Angreifer

- „Drupageddon“: Im Oktober 2014 wurde eine kritische SQL-Injection-Schwachstellen im verbreiteten CMS Drupal7 geschlossen
- Offizielle Statement von Drupal:
  - „You should proceed under the assumption that **every Drupal 7 website was compromised** unless updated or patched before Oct 15th, 11pm UTC, **that is 7 hours after the announcement**. “
  - „If you find that **your site is already patched but you didn’t do it**, that **can be a symptom that the site was compromised** - some attacks have applied the patch as a way to guarantee they are the only attacker in control of the site.“ https://www.drupal.org/PSA-2014-003
- In 7 Stunden:
  1. Erkennen der Schwachstelle aus dem Patch
  2. Entwickeln eines Exploits
  3. gezielter Angriff von Drupal7-Installationen

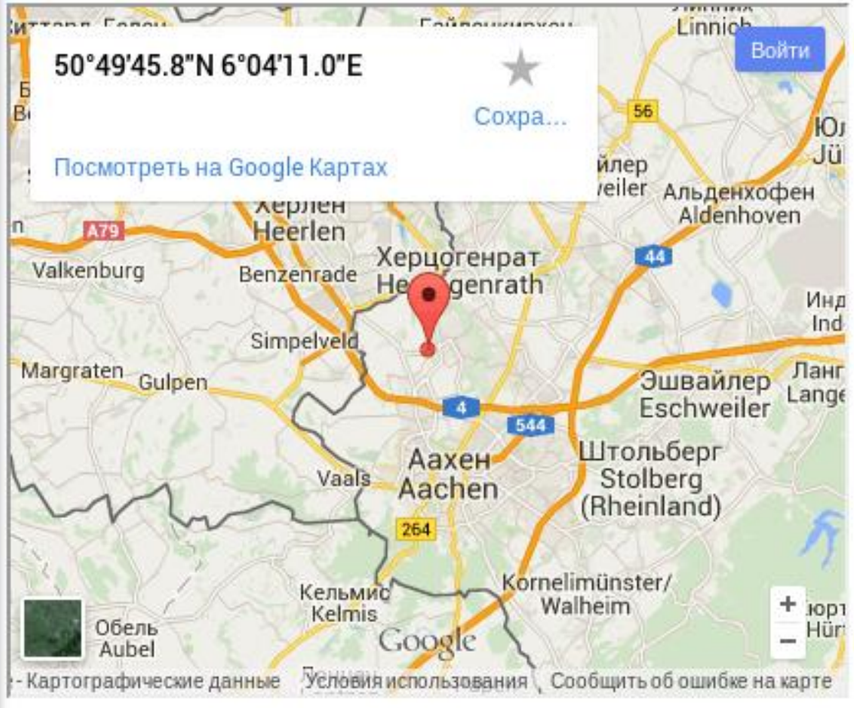
Warum Scanning?

Wirtschaftsunternehmen

- Markterhebung: Wo steht mein Produkt im Internet?
- Piraterie: Wer betreibt mein Produkt ohne Lizenz?
- Security: Wo stehen alte und anfällige Versionen meines Produkts im Internet?

United States (1757)
Japan (661)
Italy (279)
Netherlands (181)
France (168)
Germany (141)
United Kingdom (139)
Russian Federation (118)
Sweden (105)
Canada (90)
Norway (89)
Austria (85)
Spain (81)
Switzerland (79)
Czech Republic (68)
Korea, Republic Of (67)
India (64)
Poland (40)
Denmark (35)
Mexico (33)
Taiwan, Province Of (32)
Finland (30)
Argentina (26)
Brazil (25)
Viet Nam (23)
Hungary (23)

View camera online in Nordrhein-Westfalen, Bank



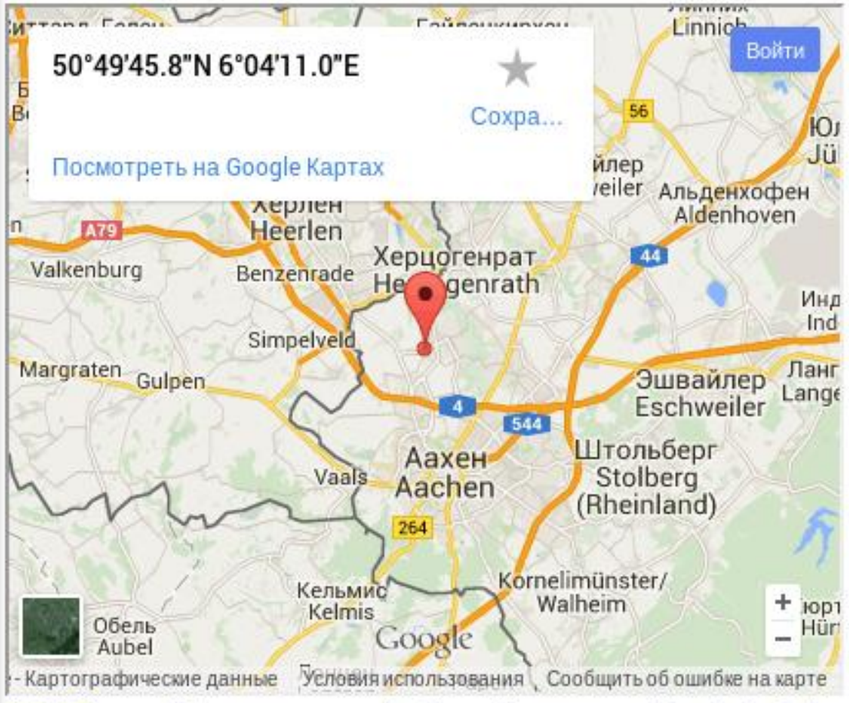
NOTE: The coordinates are very approximative and have accuracy in hundreds of miles

Country: Germany.
You can see other **online cameras** in Germany.

Country code: DE

www.insecam.org/cam/view/167411/

- Italy (279)
- Netherlands (181)
- France (168)
- Germany (141)
- United Kingdom (139)
- Russian Federation (118)
- Sweden (105)
- Canada (90)
- Norway (89)
- Austria (85)
- Spain (81)
- Switzerland (79)
- Czech Republic (68)
- Korea, Republic Of (67)
- India (64)
- Poland (40)
- Denmark (35)
- Mexico (33)
- Taiwan, Province Of (32)
- Finland (30)
- Argentina (26)
- Brazil (25)
- Viet Nam (23)
- Hungary (23)
- Indonesia (22)
- Hong Kong (21)
- Australia (21)

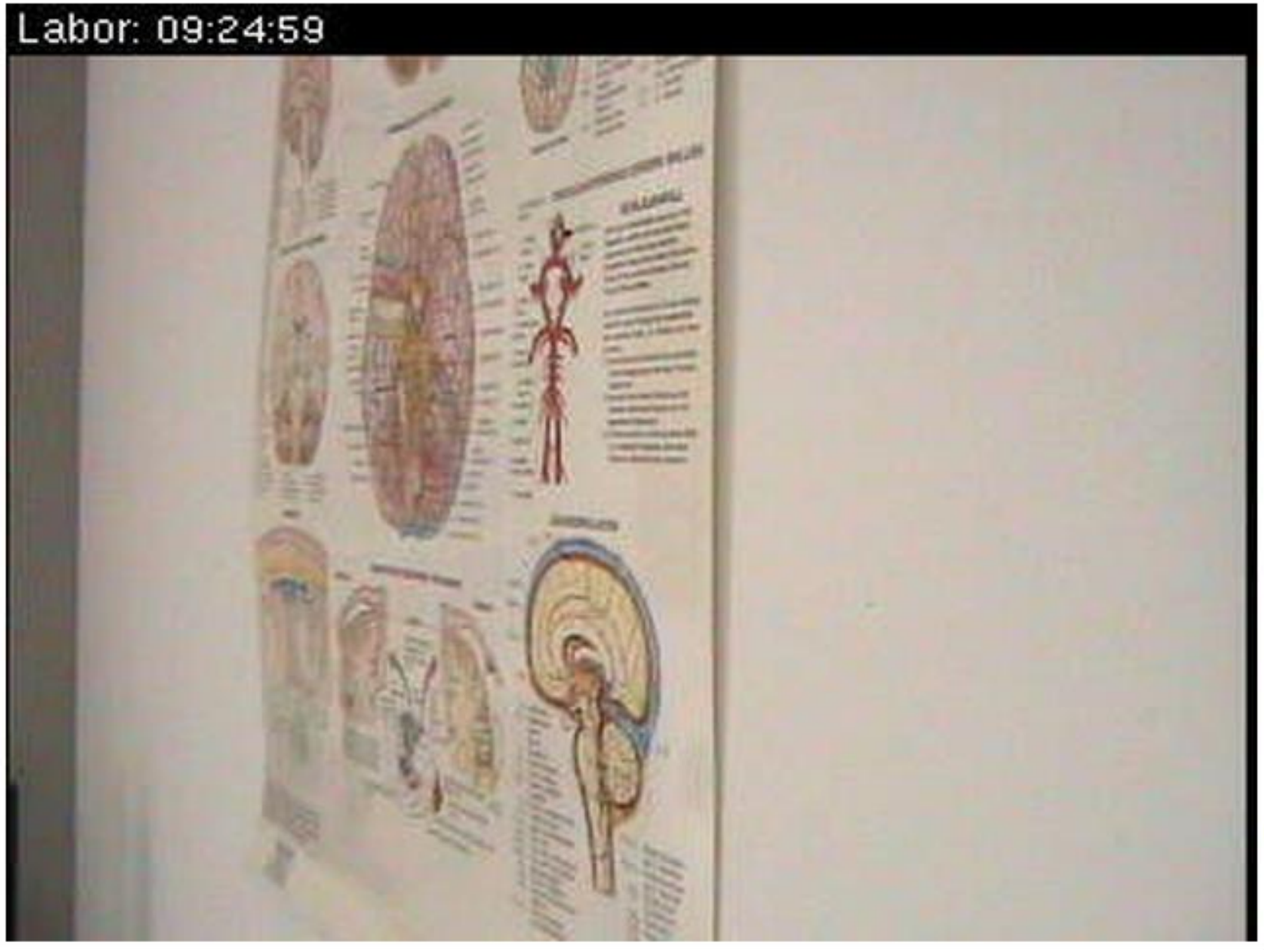


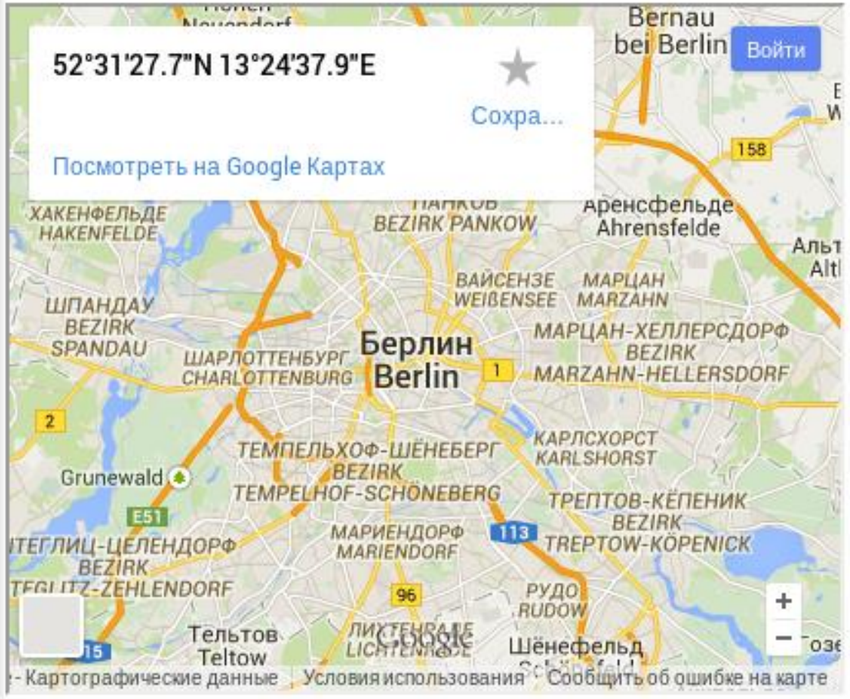
NOTE: The coordinates are very approximative and have accuracy in hundreds of miles

Country:	Germany. You can see other **online cameras** in Germany.
Country code:	DE
Region:	Nordrhein-Westfalen
City:	Bank. **View CCTV online** in Bank.
Latitude:	50.829400

www.insecam.org/cam/view/167423/

- Italy (279)
- Netherlands (181)
- France (168)
- Germany (141)
- United Kingdom (139)
- Russian Federation (118)
- Sweden (105)
- Canada (90)
- Norway (89)
- Austria (85)
- Spain (81)
- Switzerland (79)
- Czech Republic (68)
- Korea, Republic Of (67)
- India (64)
- Poland (40)
- Denmark (35)
- Mexico (33)
- Taiwan, Province Of (32)
- Finland (30)
- Argentina (26)
- Brazil (25)
- Viet Nam (23)
- Hungary (23)
- Indonesia (22)
- Hong Kong (21)
- Australia (21)
- Slovakia (19)



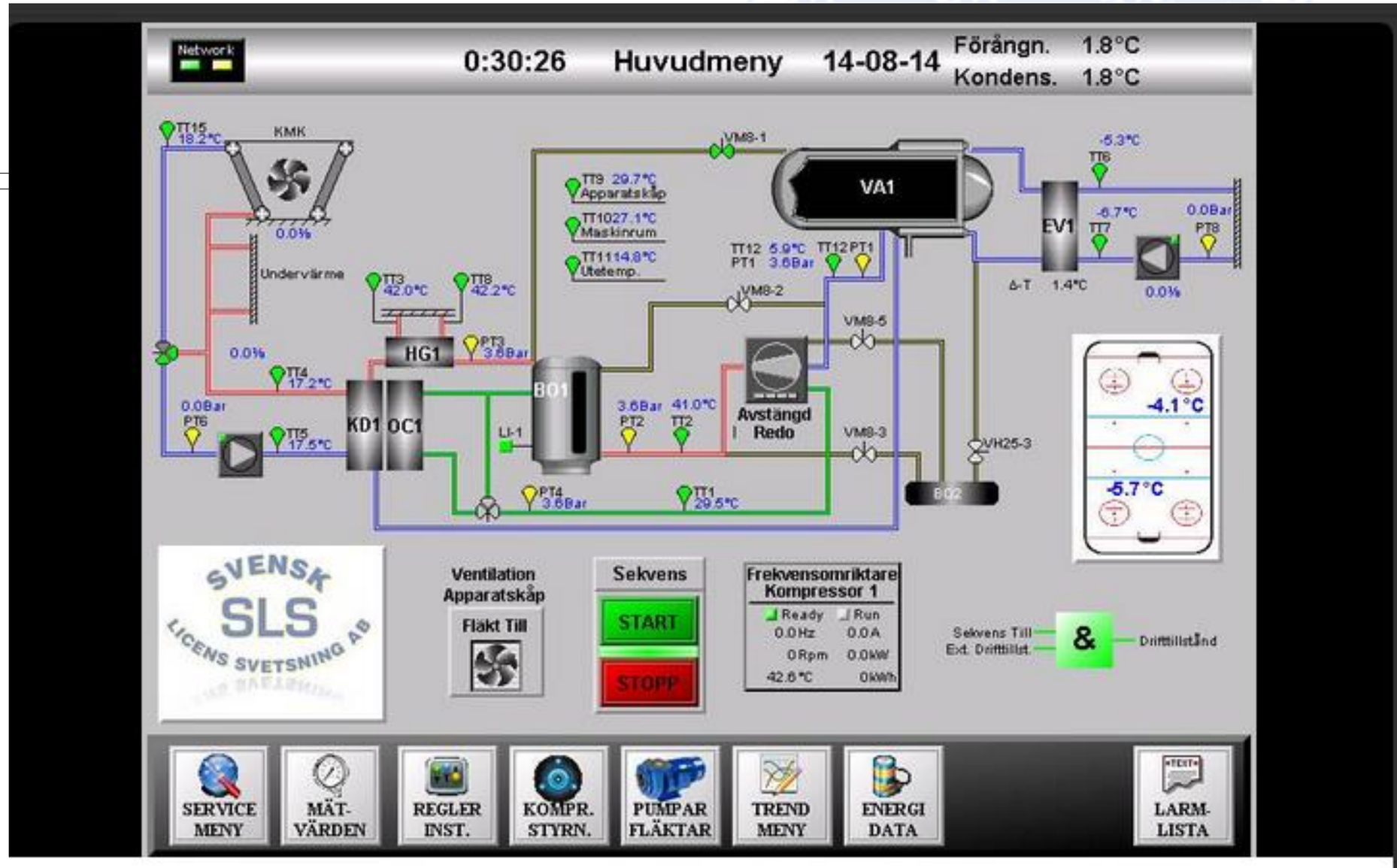


NOTE: The coordinates are very approximative and have accuracy in hundreds of miles

Country:	Germany. You can see other **online cameras** in Germany.
Country code:	DE
Region:	Berlin
City:	Berlin. **View CCTV online** in Berlin.
Latitude:	52.524370
Longitude:	13.410530

141.20.31.128

Offene VNC-Dienste im Internet (ohne Passwortschutz)

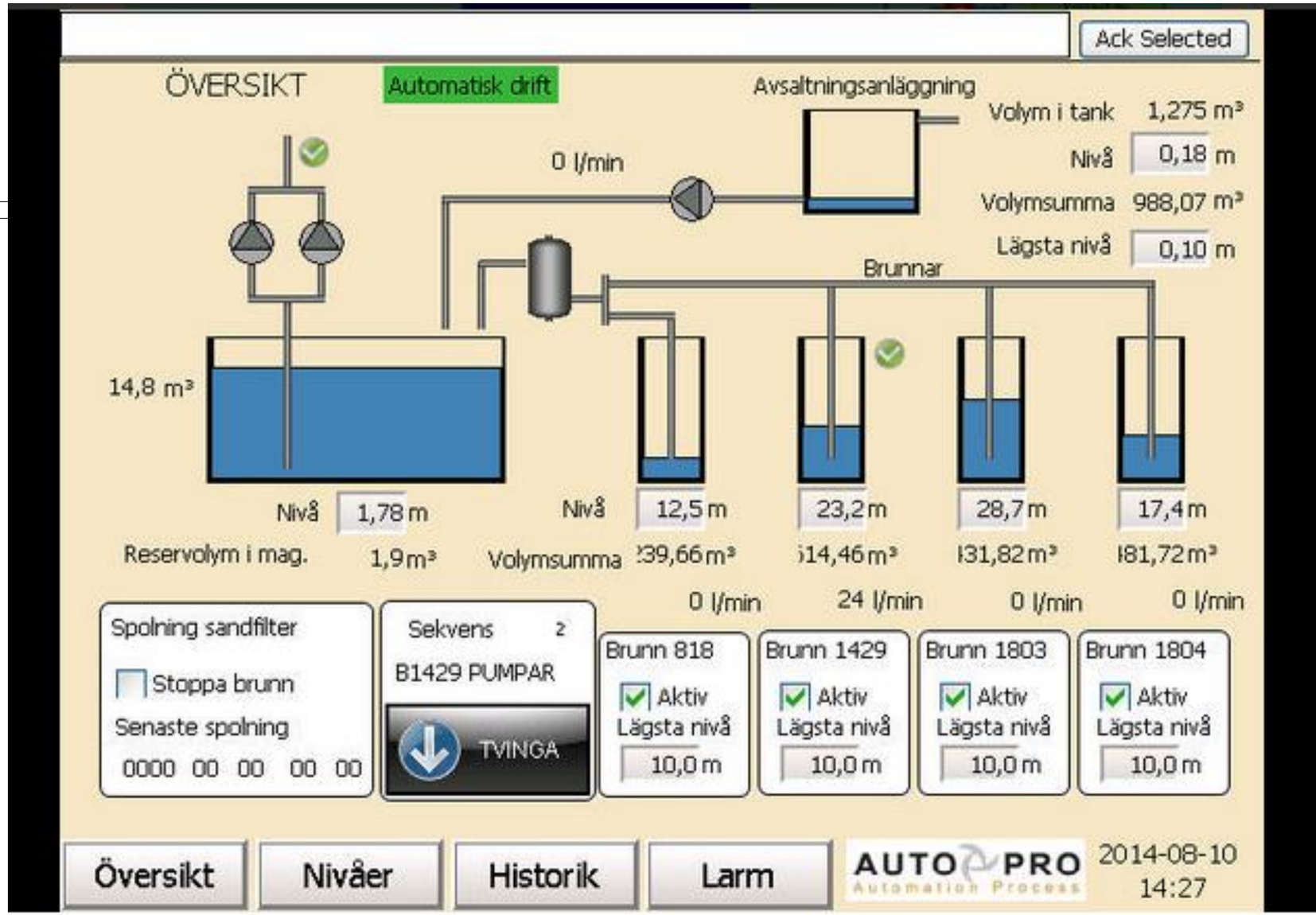


Dan Tentler @Viss · Aug 15
OH FUCK. Is this a hockey rink?! :D pic.twitter.com/NCAQfDZXim

13 18

https://twitter.com/Viss

Offene VNC-Dienste im Internet (ohne Passwortschutz)

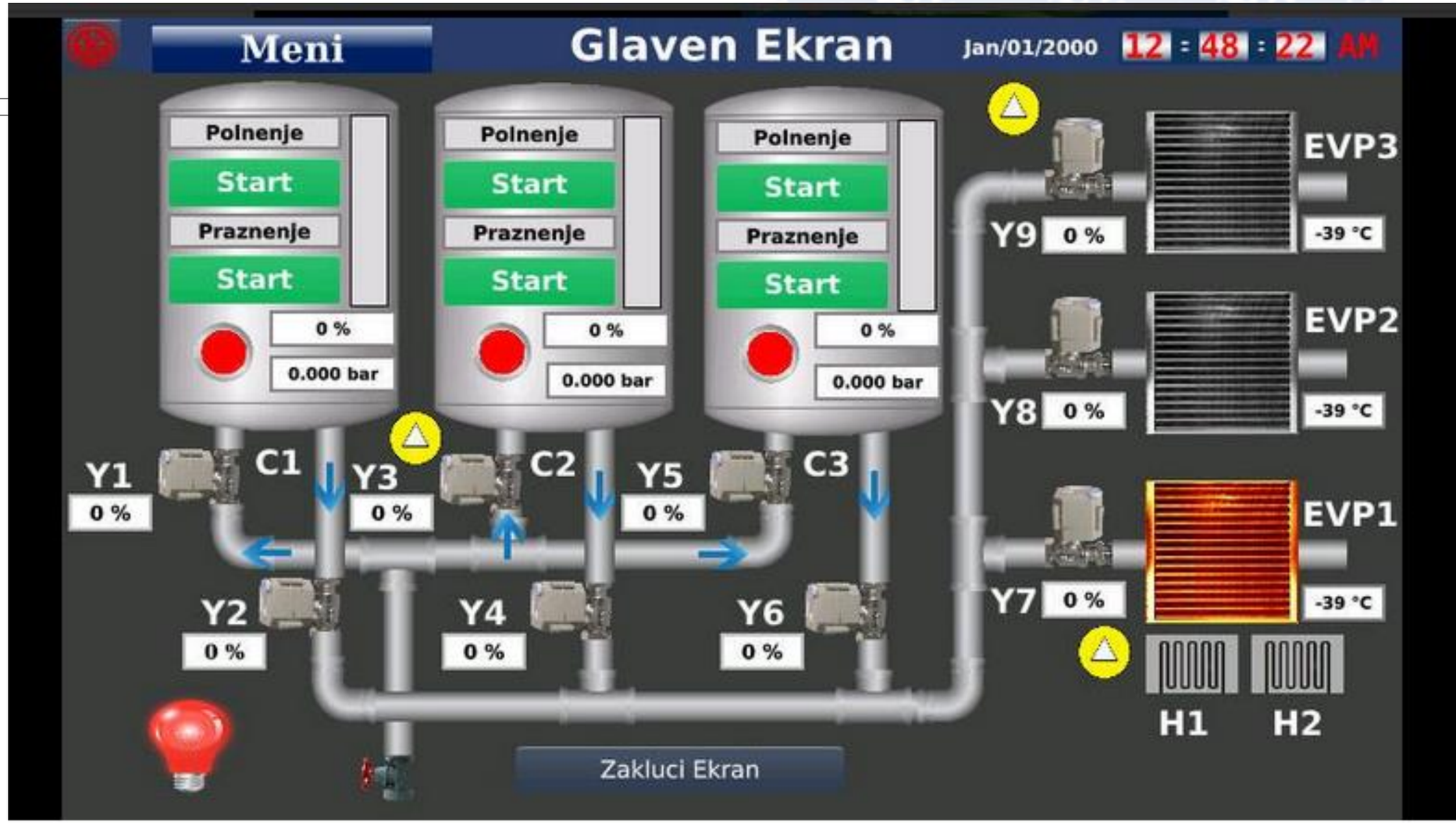


Dan Tentler @Viss · Aug 14
something else that pumps fluid around pic.twitter.com/DdkQuXdJVu

3 2

https://twitter.com/Viss

Offene VNC-Dienste im Internet (ohne Passwortschutz)



Dan Tentler @Viss · Aug 15
evaporative coolers? pic.twitter.com/28bsDJyEXt

1 5

https://twitter.com/Viss

Erfahrungen mit Scans

Rechtliches

- Nach deutschem Gesetz sind horizontale Scans nicht verboten
- Verboten ist: Umgehung von Zugangsbeschränkungen, z.B. auch:
  - Default-Passwörter
  - wirkungslose Zugangsbeschränkungen (Hidden-Links, etc.)

Ethik und Moral

- Opt-in/Opt-out: kein Äquivalent zur robots.txt für OSI-Layer 3

http://nmap.org/book/legal-issues.html

Erfahrungen mit Scans

Scanning aus dem ITS-Labor

- Bisher 20 komplette Scans (+ abgebrochene Scans)
- ~4,5 TB Netzwerkverkehr alleine durch komplette Scans
- Einige Duzend abgebrochene Scans
- Aktuell wöchentliche Scans von Port 80 und 443
  - Speichern der Response von `GET /`
  - Speichern der SSL-Zertifikate
- Fingerprinting der Dienste (welches Produkt, welche Version, welche Extensions, welche Konfiguration, ...)

Erfahrungen mit Scans

OSI Layer 3-Probleme

- Zmap schafft Scans mit 3 Gbit/s auf schneller Workstation
- Andere Netzwerkkomponenten schaffen 3 Gbit/s *nicht*
- aktuelle Scans mit ~10 Mbit/s

OSI Layer 8-Probleme

- „Ihr greift Rechner im Internet an!!1!“
- „Das ist illegal!11!!!“

Erfahrungen mit Scans

Feedback aus dem Internet

- Automatisierte Abuse-Emails aus IDS vs. persönlicher Kontakt von Admin

---

Please exclude us from your port scanner. Thank you!

128.128.0.0/16

--

****

[redacted]

Sir or Madam,

Over the last 30 days our computers have been port scanned from IP address: http://194.95.72.110/ which originates from an IP block owned by your university. We respectfully request you Blacklist our IP range immediately from all University owned or managed computers.

Blacklist IP:
10.160.0.10 – 13
10.160.1.10 - 48

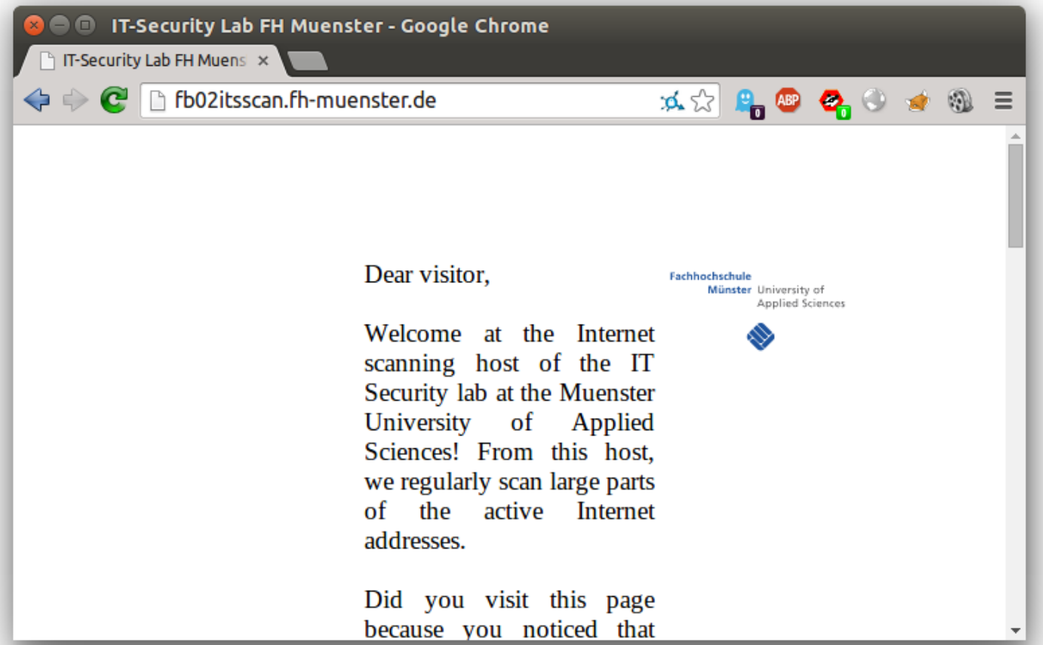
I have included our Vice President of Engineering should you have further questions and forwarded this request onto our security, compliance and legal departments.

Thank you
Chris

Erfahrungen mit Scans

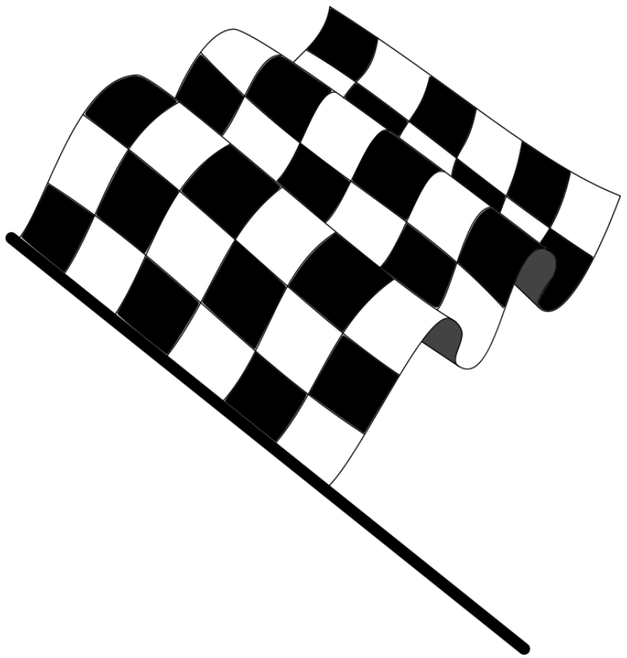
Internet-Scanning als guter Internet-Bürger

- Ankündigungen versenden, z.B. an das CERT des Providers
- Sprechenden Reverse-DNS einrichten, z.B. http://fb02itsscan.fh-muenster.de/
- Webseite auf Scanning-IP laufen lassen
  → Wer?
  → Warum?
  → Kontaktdaten (Email und Telefon)



Zusammenfassung

- Anfällige System im IPv4-Internet werden gefunden!
- Angriffe schon wenige Stunden nach Veröffentlichung von Schwachstelle
- Internetscans sollten strukturiert durchgeführt werden
- Vorhersage: IPv6 ist keine Rettung



Diskussion. Fragen.