Máte už svůj Let's Encrypt certifikát?

Ing. Tomáš Hála
IT Security & Operations manager
ACTIVE 24, s.r.o.
@tomashala

1. června 2016
Internet a Technologie 16

Už jste někdy šifrovali?

Hlava II

Nepovolené internetové hry

§ 82

Blokace nepovolených internetových her

(1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami (dále jen „seznam nepovolených internetových her“).

Svobodný INTERNET

Co jsme Ioni slibovali

Co jsme loni slibovali

- HTTPS na všech webech by default

- instalace a provoz SSL zcela zdarma

- samoobslužná instalace certifikátů

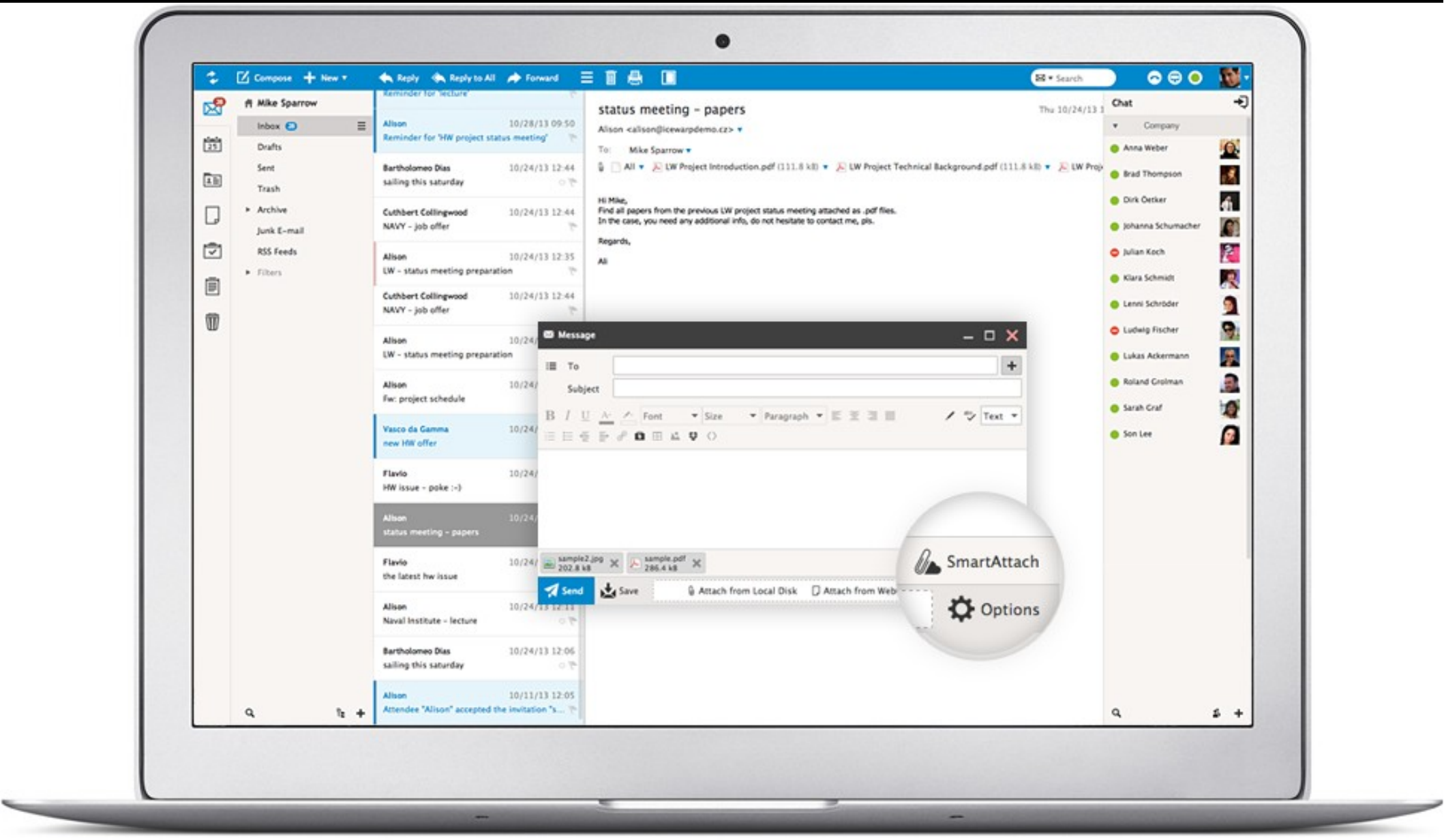
- podpora SPDY a následně HTTP/2

- podpora SSL na IPv6

- SSL terminace na reverzní proxy NGINX

Splněno! A čím dalším jsme se zabývali poslední rok?


O.K
MULDER
Erik Rotteveel
SMAAK


Compose
New
Reply
Reply to All
Forward
Search
Mike Sparrow
Inbox
Drafts
Sent
Trash
Archive
Junk E-mail
RSS Feeds
Filters
Alison 10/28/13 09:50
Reminder for 'HW project status meeting'
Bartholomeo Dias 10/24/13 12:44
sailing this saturday
Cuthbert Collingwood 10/24/13 12:44
NAVY - job offer
Alison 10/24/13 12:35
LW - status meeting preparation
Cuthbert Collingwood 10/24/13 12:44
NAVY - job offer
Alison
LW - status meeting preparation
Alison
fw: project schedule
Vasco da Gamma
new HW offer
Flavio
HW issue - poke :-)
Alison
status meeting - papers
Flavio
the latest hw issue
Alison
Naval Institute - lecture
Bartholomeo Dias 10/24/13 12:06
sailing this saturday
Alison 10/11/13 12:05
Attendee "Alison" accepted the invitation "s...
status meeting - papers
Alison <alison@icewarpdemo.cz>
To: Mike Sparrow
All
LW Project Introduction.pdf (111.8 kB)
LW Project Technical Background.pdf (111.8 kB)
Hi Mike,
Find all papers from the previous LW project status meeting attached as .pdf files.
In the case, you need any additional info, do not hesitate to contact me, pls.
Regards,
Ali
Chat
Company
Anna Weber
Brad Thompson
Dirk Oetker
Johanna Schumacher
Julian Koch
Klara Schmidt
Lenni Schröder
Ludwig Fischer
Lukas Ackermann
Roland Grolman
Sarah Graf
Son Lee
Message
To
Subject
Font
Size
Paragraph
Text
sample2.jpg 202.8 kB
sample.pdf 286.4 kB
Send
Save
Attach from Local Disk
SmartAttach
Options


inveaTECH


radware

O čem že je tato přednáška?

Let's Encrypt

Ale proč vlastně komunikaci šifrovat?

How?

Exploit the target transparently by injecting a browser-based exploit while he's surfing the web (http)

AT&T caught injecting extra ads on airport WiFi hotspot

1

Adam Westlake - Aug 26, 2015

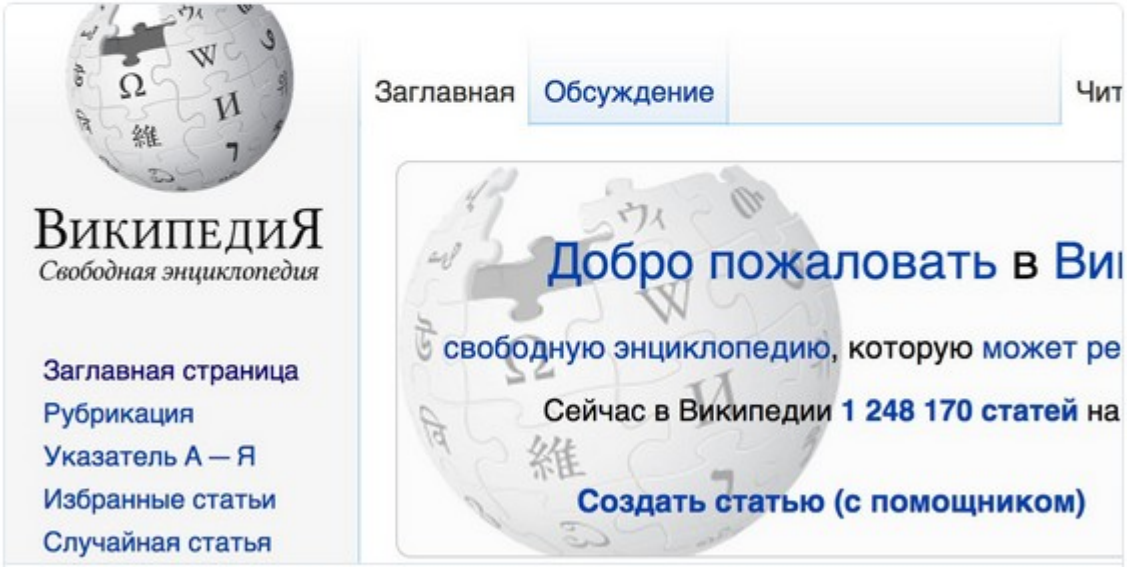
It seems AT&T may be tampering with mobile users' internet traffic for their own benefit on their "free" public WiFi hotspots. The company's hotspot at the Dulles International Airport in Virginia was found to be using ad-injecting code to deliver more advertisements to users while they browse the web. Stanford lawyer and computer scientist Jonathan Mayer made the discovery, detailing the tactic on his blog *Web Policy*.

“Eric” “Mill”
@konklone

Sledovat

Wikipedia's decision to enforce HTTPS is now pitting them against Russian censors, who want the HTTPS turned off: theguardian.com/world/2015/aug…

Zobrazit překlad



Russia briefly bans Wikipedia over page relating to drug use

Court ordered ban on page about charas, an Indian form of hashish, but some Russian users found entire site blocked due to secure https protocol

theguardian.com


Pineapple Juice 4000

Jak jsme Let's Encrypt implementovali v ACTIVE 24

Jak jsme Let's Encrypt implementovali v ACTIVE 24

- na každou doménu na našem Linux hostingu
- zdarma a automaticky krátce po zřízení hostingu
- včetně aliasů, mimo wildcard (např. *.active24.cz)
- samozřejmě automatické obnovy
- při zřízení self-signed, následně nahrazování pomocí LE
- možnost nahradit certifikátem komerčním
- služba typu „best-effort“
- vybrali jsme acme.sh klient

A co vy, máte už svůj Let's Encrypt certifikát?

WANTED

- senior J2EE programátor
- BSD server administrátor

active 24

Děkuji za pozornost!

www.active24.cz
blog.active24.cz
@active24cz
@tomashala