Securing Identities in a Zero Trust World

Lidé jsou nepoučitelní. Nejčastější slabá hesla wi-fi routerů roku 2020

1. září 2020 10:01

Analytici společnosti ESET naskenovali více než sto tisíc routerů v německých sítích a vytvořili seznam nejčastěji používaných hesel. Ta výchozí, která nemají žádný bezpečnostní efekt, samozřejmě vedou. My vám poradíme, jak router zabezpečit správně.

To jsou zase hesla ...

Thales Security Leader

Tomáš Jilík, Petr Kunstát

THALES

Thales Group Focuses on Intelligent Systems

- €19b revenue
- 80,000 employees
- 68 countries
- €1b R&D investment

Aeronautics | Space | Ground transportation | Defence | Security

Hardware Security Modules	Advanced defence systems	Air Traffic Management	In-flight entertainment	Space solutions	Rail signalling and supervision	Flight avionics
#1	#1	#1	#2	#2	#2	#3
worldwide	in Europe for defence sensors and mission systems	worldwide	worldwide	worldwide (civil satellites)	worldwide	worldwide

THALES

THALES

Zero Trust

Zero Trust - Why we should care

Organizations should **not** automatically **trust anything** *inside* **or** *outside* their perimeters.

Enterprises should leverage flexible security applied at the app level based on **users**, their **locations** and other data to establish trust for entities seeking access to a particular part of the enterprise.
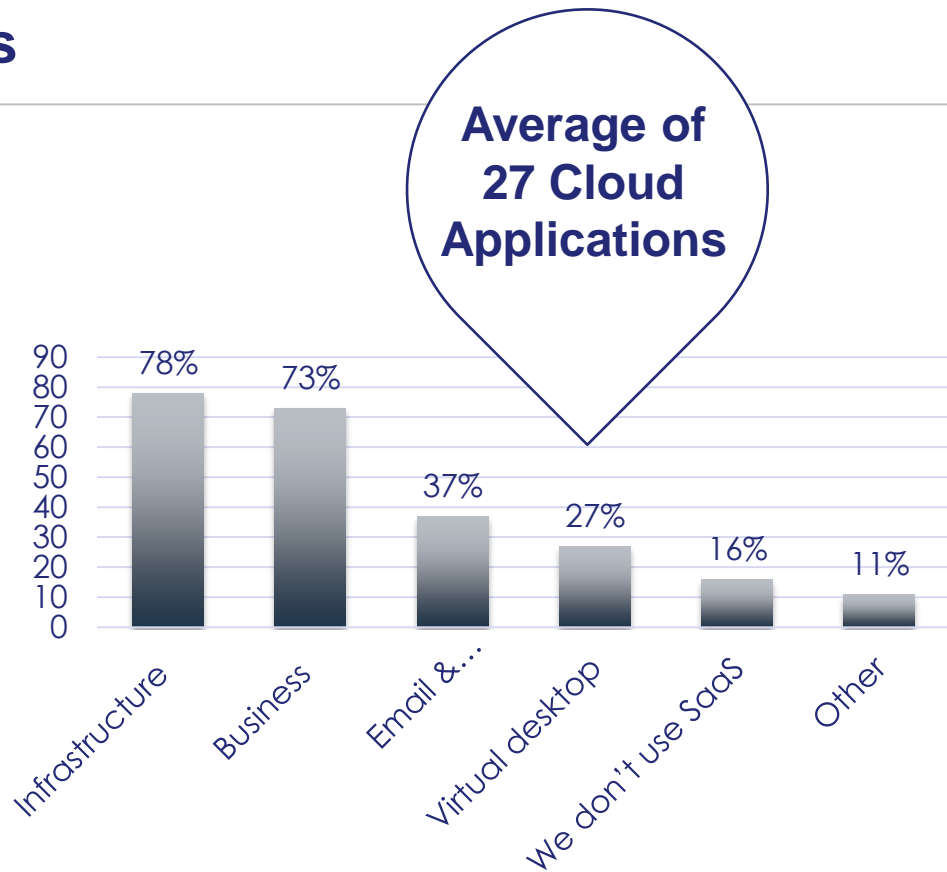
Rather that trusting the network to any extent, a zero-trust model puts all of its effort behind protecting **applications**, and the **data** they **access.**

THALES

The main cause of data breaches

IDENTITY THEFT

80% of breach incidents came from identity theft

Average of 27 Cloud Applications

Chart (values by category):
- Infrastructure: 78%
- Business: 73%
- Email &…: 37%
- Virtual desktop: 27%
- We don't use SaaS: 16%
- Other: 11%

THALES

Passwordless

The problem with passwords

THREAT

'123456789'
'password'

Most popular passwords

80%

Data breaches related to passwords

COST

40%

Helpdesk calls are password related

HASSLE

130

Accounts associated with an email address

62%

Users reuse password across accounts

THALES

Problem with the Password -> Password Fatigue

▌ **What is it ?....**

▌ **When users are asked to remember an excessive number of passwords as part of their daily routine, they begin to get frustrated and lazy about creativity.**

▌ **A password for the PC**

▌ **Bike lock, PIN , Bank PIN …**
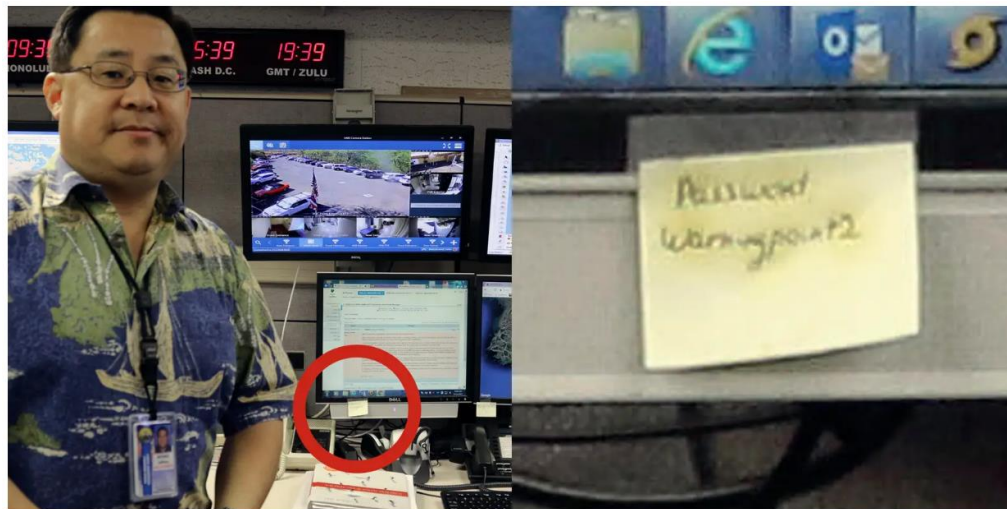
Hawaii Emergency Management Agency.

THALES

Why passwordless authentication ?

More Security

Eliminate phishing, credential stuffing & other passwords related attacks

Less Friction

No need to **remember** multiple passwords. Faster & seamless login.

Lower TCO

Reduce
IT operations **costs** & support costs

THALES

Lazy Phi$hing

Lazy Phi$hing

- **Phishers, are trying to phi$h with dynamite.**

- **Clone default Office365 login page.**

- **Once user enters in e-mail address, they are redirected to a non-branded login page**

THALES
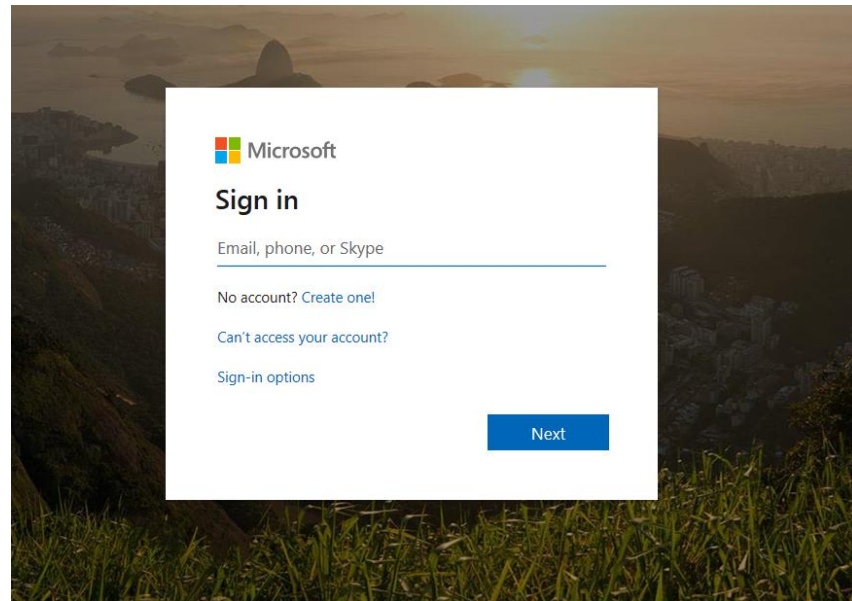
Lazy Phi$hing…harder to Phish with customized logon pages !

▌ **Customize your logon page with Office365.**

▌ **Users will feel much more comfortable entering credentials.**

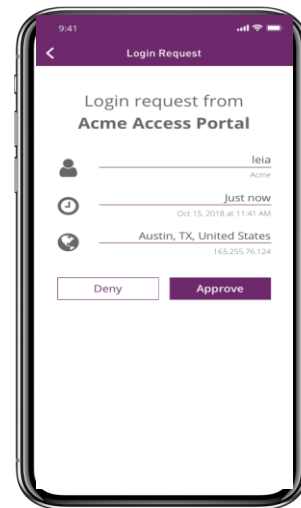▌ **It lets your users know they are visiting a legitimate login page.**
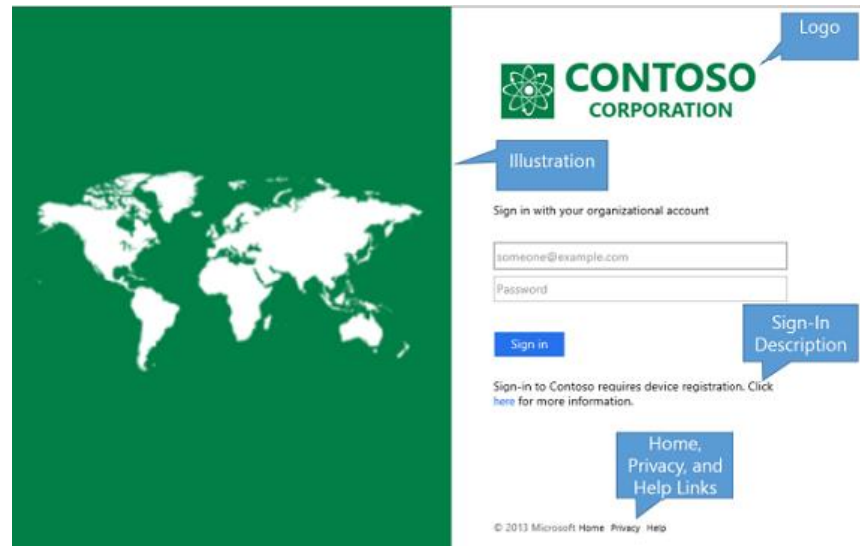
"Jim, are you on a logon page that
has our green CONTOSO Corporate logo on it ?

THALES

SafeNet Trusted Access

SMS

Biometric

OTP Push

Hardware

PKI
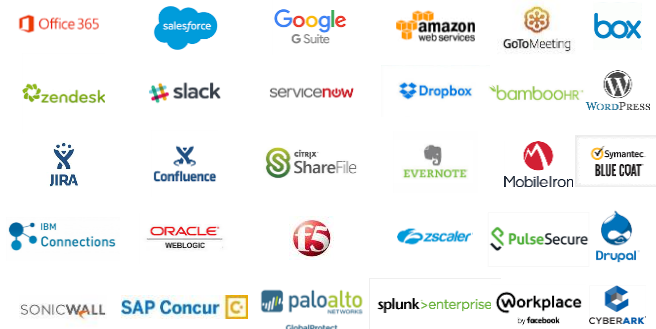
1

IDENTIFY

Validate user's identity

3

APPLY

Apply appropriate access controls, with smart single sign on

2

ASSESS

Assess which access policy should be applied

SafeNet Trusted Access allows organizations to manage access to cloud applications by validating identities, determining levels of trust and applying appropriate access controls each time the user accesses a cloud service.

THALES

Create a standard RISK profile for different applications

LOW Risk Login policy created in the THALES Safenet Trusted Access

Low RISK Login ⓘ   ✏ Edit

Conditions ⓘ

When an access attempt occurs under all of the conditions

📶 Network- Inside these networks ⌄

💻 User Device ⌄

⚙ Operating System- Listed ⌄

📍 User Location- From these Countries ⌄

🛬 Country Change ⌄

Requirements ⓘ

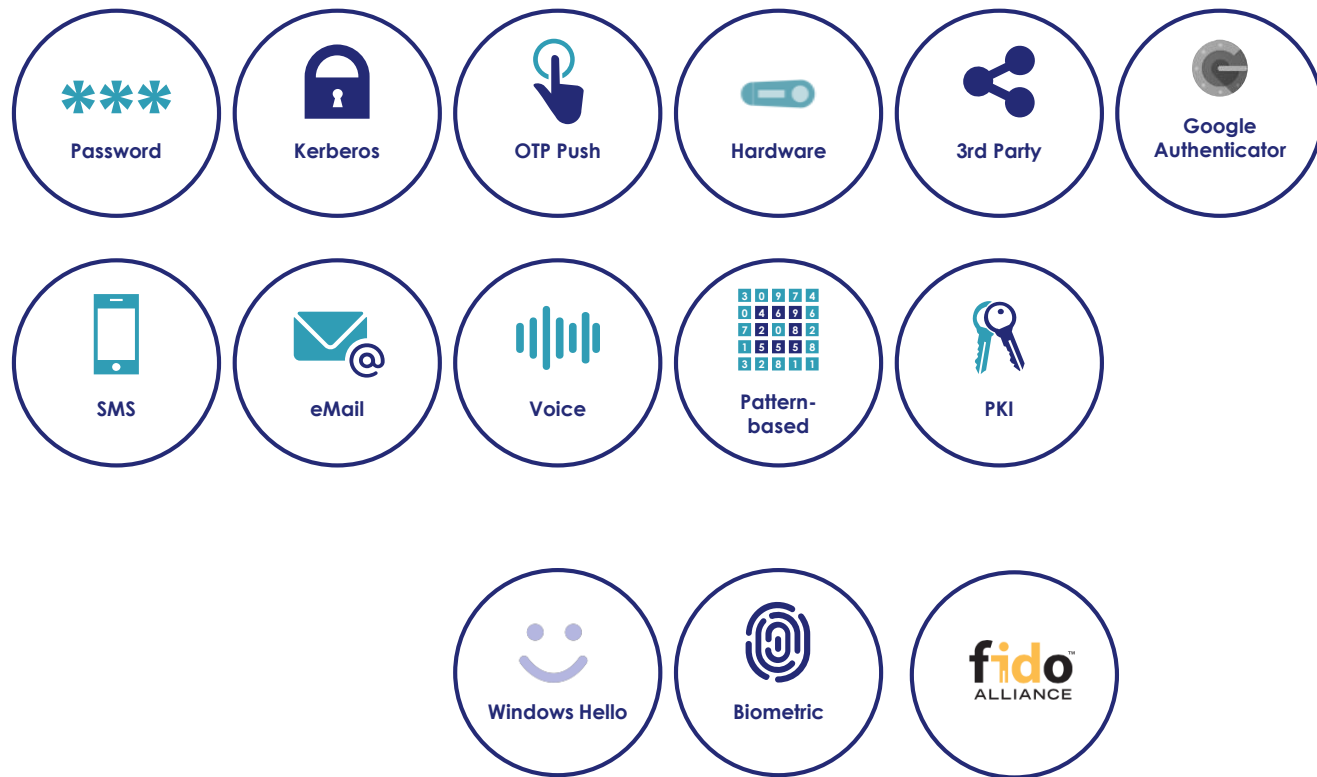Then access is

Granted

After authenticating with

Password ⓘ
     Once per session

Token Based Authentication (OTP) ⓘ
     Every access attempt

THALES

Universal Authentication

Single Factor   Multi-factor   Passwordless   Adaptive

Password

Kerberos

OTP Push

Hardware

3rd Party

Google Authenticator

SMS

eMail

Voice

Pattern-based

PKI

Windows Hello

Biometric

fido ALLIANCE

Utilize the MFA schemes already deployed

Extend PKI authentication to the cloud

Offer the appropriate level of assurance
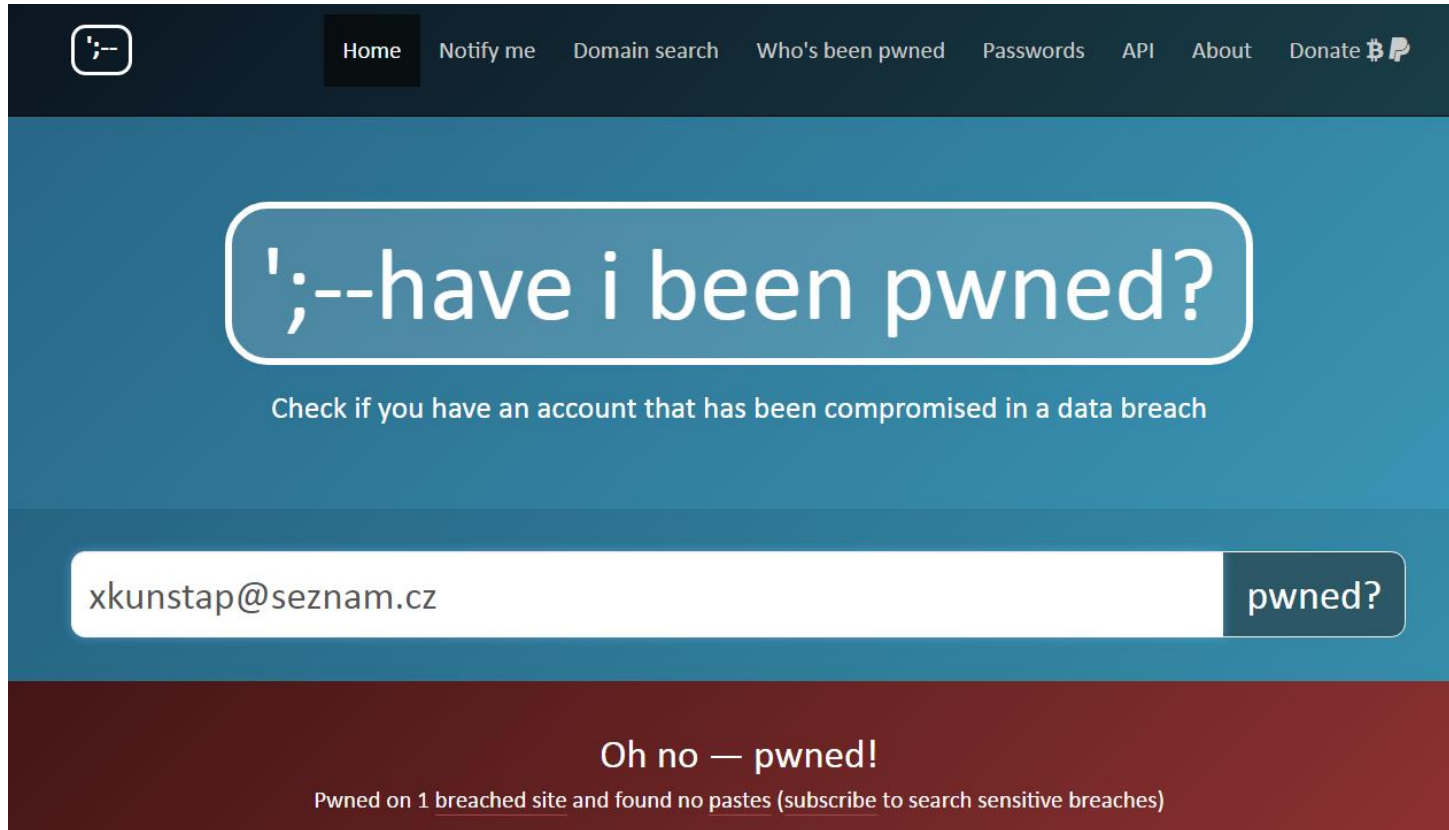
Offer convenience with Passwordless authentication

15

THALES

SafeNet eToken FIDO2 USB token and IDPrime FIDO2 smartcards

- **SafeNet FIDO devices**
  - Supports all PKI use cases
  - FIDO/CTAP (2.0/2.1) compliant and certified (functional and security certifications)
  - SC NFC interface: PKI & FIDO in either contact & contactless mode

Do you dare to check?

THALES