Silne uwierzytelnianie w aspekcie nadchodzących regulacji, ostatnich incydentów cyberbezpieczeństwa oraz bieżącego orzecznictwa

Krzysztof Góźdź – Sales Manager, krzysiek@secfense.com

SECFENSE

SECFENSE

Kim jesteśmy?

- Eksperci w kwestii **ochrony cyfrowej tożsamości użytkownika**
- Członek **FIDO Alliance**, partner Yubico, Google, EY, NVIDIA
- Laureat nagród, m.in. Gazety Bankowej, Rzeczpospolitej czy **Banking i Insurance Forum**
- Dostawca rozwiązań w zakresie silnego uwierzytelniania głównie do dużych i mniejszych **banków**, branży **ubezpieczeniowej** oraz **administracji** publicznej

SECFENSE

Plan na najbliższe 19 minut

1. **Regulacje** w zakresie silnego uwierzytelniania
2. Ostatnie **incydenty** dot. bezpieczeństwa systemów **VPN**
3. Orzecznictwo ws. **wycieków danych osobowych**
4. **Passkeys** – nadchodzące remedium na ww. problemy

SECFENSE

1. Regulacje w zakresie silnego uwierzytelniania

KOMISJA EUROPEJSKA

Bruksela, dnia 24.9.2020 r.
COM(2020) 595 final

2020/0266 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014

(Tekst mający znaczenie dla EOG)

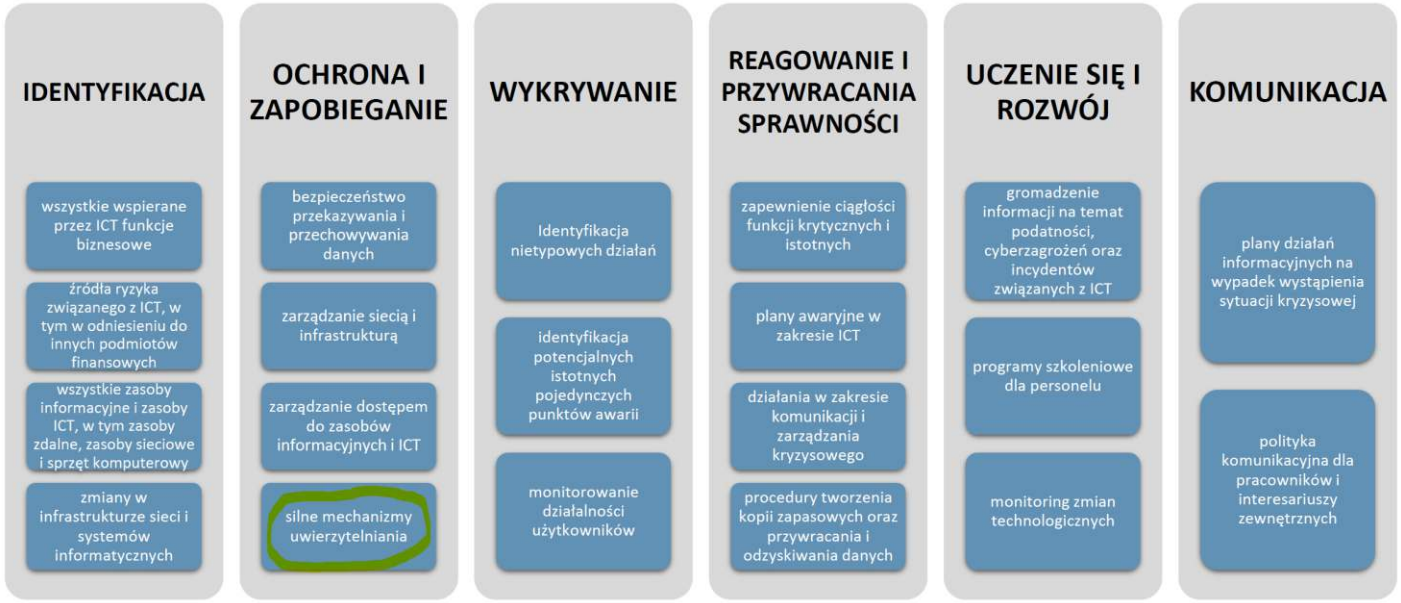
Artykuł 8

Ochrona i zapobieganie

4. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, podmioty finansowe:

d) wdrażają polityki i protokoły dotyczące silnych mechanizmów uwierzytelniania, oparte na odpowiednich normach i specjalnych systemach kontroli, aby uniemożliwić dostęp do kluczy kryptograficznych, dzięki którym dane szyfruje się na podstawie wyników zatwierdzonych procesów klasyfikacji danych i oceny ryzyka;

DORA | Zarządzanie ryzykiem ICT



Źródło: Kancelaria DZP, Paweł Rudolf, Forum Technologii Bankowości Spółdzielczej 2023

DZP

1. Regulacje w zakresie silnego uwierzytelniania

a) Czy DORA i NIS 2 wymuszają na objętych regulacjami organizacjach wdrożenie silnego uwierzytelniania w stosowanym przez nich systemach cyfrowych?
b) Czy mechanizmy silnego uwierzytelniania powinny zostać wdrożone bezwzględnie do wszystkich rodzajów systemów cyfrowych?
c) Czy użycie określenia "*cryptographic keys*" lub "*klucze kryptograficzne*" oznacza, że jako mechanizmy silnego uwierzytelniania nie mogą być wykorzystywane metody inne, niż oparte na kryptografii asymetrycznej, która to właśnie wymaga ww. kluczy?
d) Jakie organizacje są objęte każdą z tych regulacji?
e) Kim jest "*ICT third-party providers*" na gruncie DORA? Czy jest to każdy dostawca usług i technologii informatycznych? Czy objęci DORA dostawcy również powinni stosować u siebie mechanizmy silnego uwierzytelniania?
f) Co konkretnie oznacza tzw. "*size-cap rule*" na gruncie regulacji NIS 2? Jak organizacja ma się dowiedzieć, czy podlega tej regule?
g) Kto na gruncie regulacji NIS 2 i DORA odpowiada za ich wdrożenie?
h) Jakie są sankcje za złamanie przepisów regulacji DORA i NIS 2? Kto personalnie je ponosi?

SECFENSE

2. Ostatnie incydenty dot. bezpieczeństwa systemów VPN

SECFENSE

2. Ostatnie incydenty dot. bezpieczeństwa systemów VPN

KAPITAN HACK.PL

HOME POSTY WIDEO KAMPA

Fortinet z kolejną krytyczną podatnością RCE. Dotyka SSL VPN i jest aktywnie wykorzystywana przez atakujących

13 lutego 2024

EXPLOIT FORTIGATE FORTINET

KAPITAN HACK.PL

HOME POSTY WIDEO KAMPA

Uwaga na te krytyczne podatności w Cisco oraz Fortinet – dzięki nim haker może włamać się do Twojej firmy

20 lutego 2023

BUG CISCO CVE FORTINET VULNERABILITY

sekurak

SZKOLENIA | KSIĄŻKA | AKTUALNOŚCI | TEKSTY | KONTAKT |

Żądny wiedzy? Wbijaj na **Mega Sekurak Hacking Party** w maju! -30% z ko

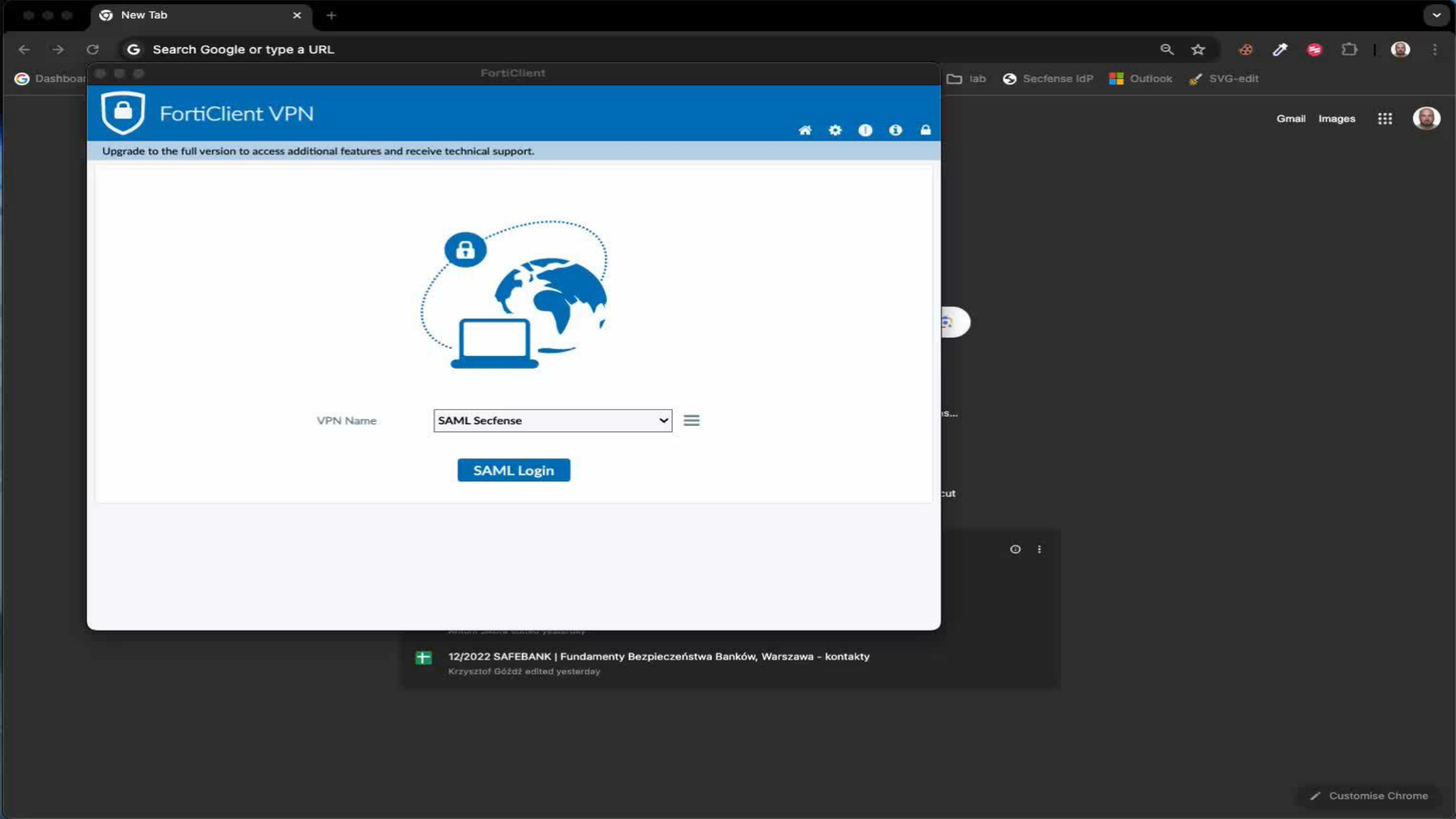
Krytyczny oday w VPN od PaloAlto (podatność jest wykorzystywana w realnych atakach). CVSS 10/10.

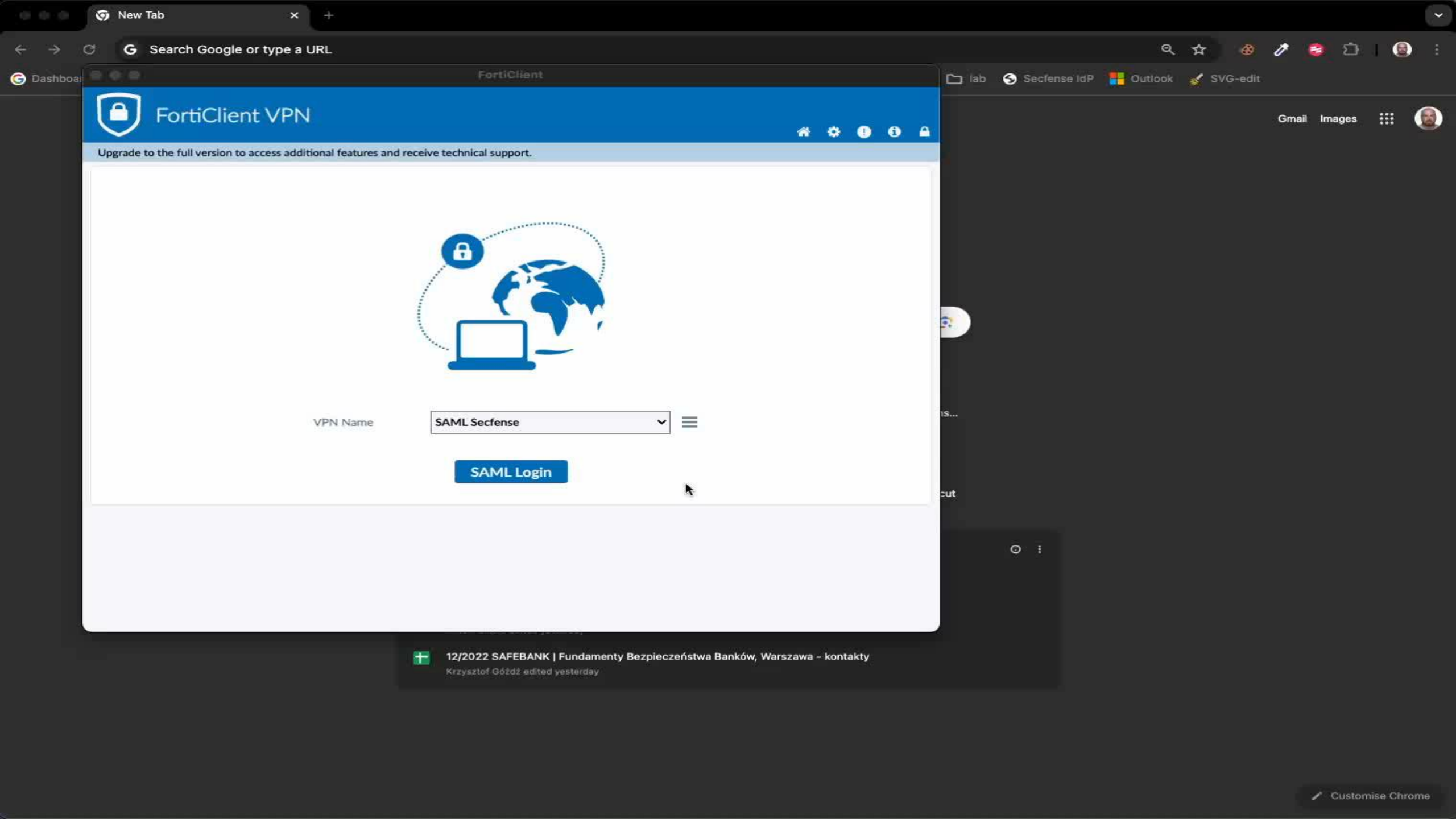
12 KWIETNIA 2024, 12:33 | W BIEGU | KOMENTARZY 12

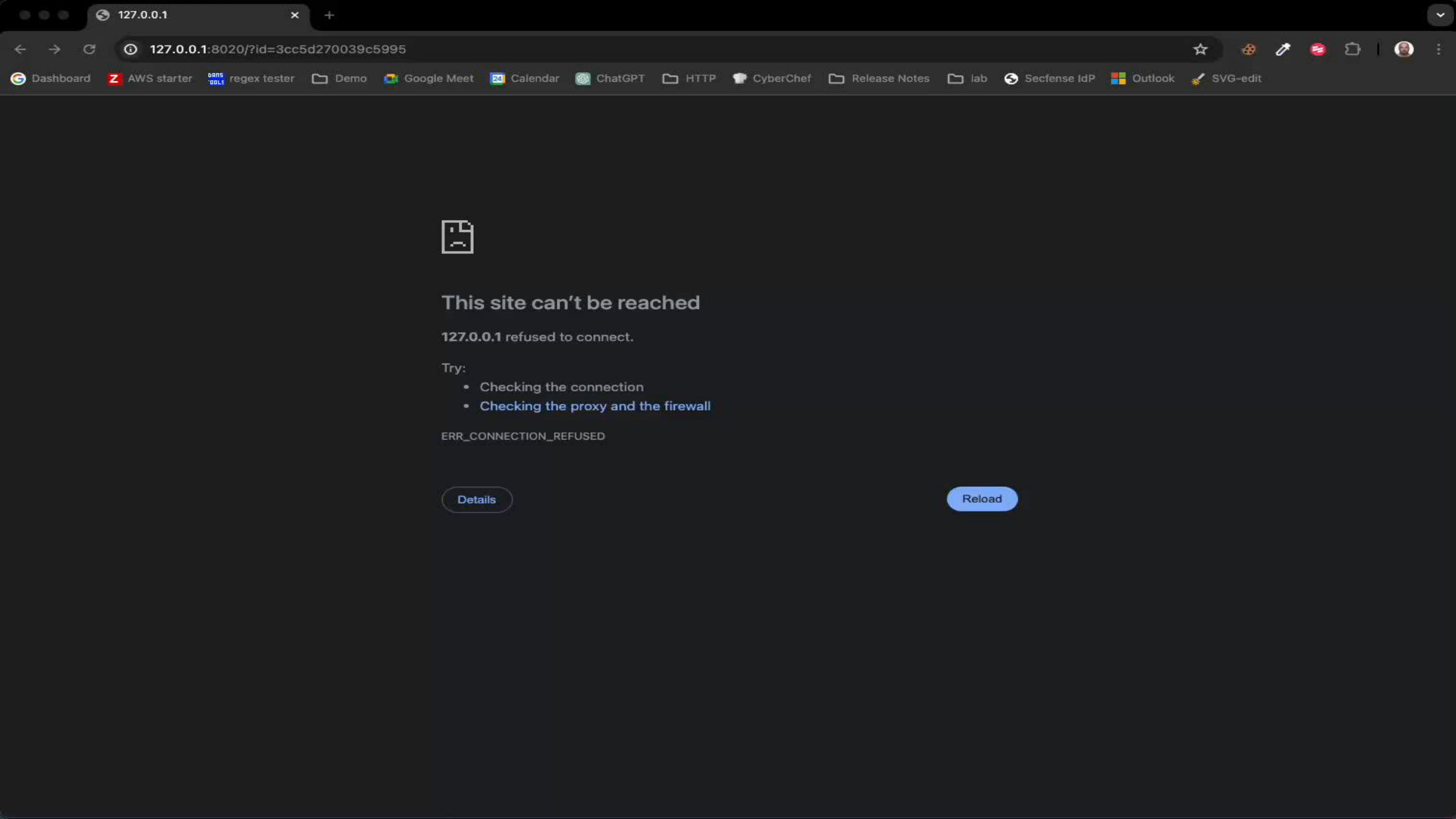
TAGI: COMMAND INJECTION, PALOALTO

Podatny jest GlobalProtect. „GlobalProtect is more than a VPN. It provides flexible, secure remote access for all users everywhere."

Podatność umożliwia zdobycie roota na urządzeniu PaloAlto – bez konieczności jakiegokolwiek uwierzytelnienia (!). Unauth Command Injection. Producent informuje, że luka jest wykorzystywana w realnych atakach.


New Tab
Search Google or type a URL
Dashboar
lab
Secfense IdP
Outlook
SVG-edit
Gmail
Images
FortiClient
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
VPN Name
SAML Secfense
SAML Login
12/2022 SAFEBANK | Fundamenty Bezpieczeństwa Banków, Warszawa - kontakty
Krzysztof Góźdź edited yesterday
Customise Chrome


New Tab
Search Google or type a URL
FortiClient
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
VPN Name
SAML Secfense
SAML Login
Gmail
Images
12/2022 SAFEBANK | Fundamenty Bezpieczeństwa Banków, Warszawa - kontakty
Krzysztof Góźdź edited yesterday
Customise Chrome


127.0.0.1
127.0.0.1:8020/?id=3cc5d270039c5995
Dashboard
AWS starter
regex tester
Demo
Google Meet
Calendar
ChatGPT
HTTP
CyberChef
Release Notes
lab
Secfense IdP
Outlook
SVG-edit
This site can't be reached
127.0.0.1 refused to connect.
Try:
Checking the connection
Checking the proxy and the firewall
ERR_CONNECTION_REFUSED
Details
Reload

3. Orzecznictwo ws. wycieków danych osobowych

- **Morele.net vs. UODO**, dane ok. 2.2 mln osób, ok. 2.8 mln PLN kary
- **Odwołanie** sklepu **do NSA**, który orzekł, że „*włamanie, nie jest dowodem na to, że administrator danych nie dochował odpowiednich standardów*”
- **Jakie** więc **środki** techniczne i organizacyjne należy **stosować**?

Law4Tech

secfense.com/pl/biuletyn

4. Passkeys – nadchodzące remedium na ww. problemy

- **FBB 2023**: „*Czy klucze U2F staną się powszechną metodą uwierzytelniania w banku?*”
- **Passkeys** – opracowany przez FIDO Alliance nowy otwarty standard uwierzytelniania, w którym uwierzytelniaczem jest komputer, telefon czy klucz sprzętowy, a wygenerowane klucze kryptograficzne mogą być przenoszone pomiędzy urządzeniami
- **Jesteśmy gotowi** do implementacji passkeys w organizacji, rozmawiamy o pilocie z jednym z dużych banków

Secfense

Konto klienta | Rankomat

rankomat.pl/konto/login

Dashboard AWS starter regex tester Demo Google Meet Calendar ChatGPT HTTP CyberChef Release Notes lab Secfense IdP Outlook SVG-edit

rankomat.pl

Zaloguj się

Hej, witamy ponownie! Zaloguj się, aby kontynuować

Adres e-mail

Hasło

Zapamiętaj mnie

Nie pamiętasz hasła?

Zaloguj się

Jesteś tu nowy? Utwórz konto

SECFENSE

Zapraszamy do stoiska