

KIBERNETINIO SAUGUMO RIZIKOS  
PASIRUOŠIMAS. ĮSILAUŽIMO ATVEJAI.  
KRIZĖS. REPUTACIJOS KAINA

# Kibernetinio saugumo mokymai

2024.05.17 Online

Pakalbėkime apie įsilaužėlius, vandens potvynius ir gaisrus serverinėse ir duomenų centruose, kaip apsisaugoti, atsargines kopijas ir geriausią verslo tęstinumo planą

# Hackeriai. Duomenų nutėjimas

Lietuvos atvejai

Plastinės chirurgijos klinikos

CityBee

Elektroninės parduotuvės, bankai (EMI, Revolut)

Narystės svetainės

Skelbimai

Užsienio reikalų ministerijos ir ambasadų darbuotojų susirašinėjimo duomenys

# Hackeriai. Duomenų šifravimas

Lietuvos atvejai

Medicinos įstaigos

Medicinos elektroninė parduotuvė

Metalo gamybos įmonė

Medicinos preparatų gamybos verslas Latvijoje

# Duomenų centrai. Užpylimas vandeniu

- Vandens potvynio atvejis Nacionaliniame registrų centre Vilniuje. 2020
- Registrų centras: didžioji dalis liūties padarinių pašalinta
- Antradienio rytą didžioji dauguma Registrų centro tvarkomų registrų ir informacinių sistemų vėl pradėjo veikti po pirmadienio vakaro liūties padarinių. Tačiau kai kurie pažeidimai vis dar šalinami, siekiant kuo greičiau atnaujinti e. sveikatos sistemos ir kitų registrų darbą.
- Pirmadienio vakarą sostinę užklupusios stiprios liūties metu į Registrų centro patalpas V. Kudirkos gatvėje prasiskverbė vanduo. Dėl to sutriko ten esančių serverių darbas ir laikinai nebuvo galima naudotis įmonės tvarkomais registrais ir informacinėmis sistemomis.
- Registrų centro komanda visą naktį dirbo šalindama liūties padarinius ir sugebėjo atkurti daugumos registrų ir informacinių sistemų veikimą. Dabar veikia Gyventojų registras, Nekilnojamojo turto registras, Adresų registras ir elektroninių aukcionų portalas.
- Tačiau Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (ESPBI IS, arba e. sveikata) atkūrimas užtruko ilgiau nei planuota, sutrikimų užfiksuota Hipotekos registre ir Turto arešto aktų registre, o klientai laikinai negali naudotis Registrų centro savitarna.
- Paslaugos ir duomenys atkurti tik per 30 dienų.

# Duomenų centrai. Vanduo ir potvyniai

## Rizikos valdymas

- Duomenų centrai turi būti statomi 2 aukšte ir aukštesniuose aukštuose DC pastatuose nėra komunalinių vamzdinių. Gėsinimas tik dujomis
- Aušinimo vandeniu problemos



# Duomenų centrai. Ugnis

- Nepasitikėkite duomenų saugyklomis ir pakopų politika, patikrinkite save du kartus
- Gaisras "OVHcloud" duomenų centre Strasbūre, Prancūzijoje



# PARTAGE D'EXPÉRIENCE


Service "Risques technologiques et particuliers" - Bureau RETEX

Feu de " Data center " - " OVH - Cloud "



# OVHcloud datacenter 'lacked' automatic fire extinguishers, electrical cutoff

Firefighters' report: Wooden ceiling rated to resist blaze for an hour

 [Thomas Claburn](#)

Tue 22 Mar 2022 // 19:16 UTC

The OVHcloud datacenter in Strasbourg, France, that was destroyed in a fire last year had no automatic fire extinguisher system nor an electrical cutoff mechanism, according to a report from the Bas-Rhin fire service.

The incident report was obtained and published by Journal du Net ([JDN](#)), a French-language IT site. It describes several issues that contributed to the destructiveness of the blaze, including the presence of toxic fumes from lead batteries, a wooden ceiling rated to resist fire for only an hour, and two inner courtyards that acted as "fire chimneys."

The fire occurred at 0046 on March 10, 2021 and destroyed SBG2, a five-story datacenter occupying 500m2. Servers in adjacent buildings SBG1 were also damaged in the incident while SBG3 and SBG4 remained operational.

"We have a major incident on SBG2," said OVH founder and chairman Octave Klaba via Twitter at the time. "The fire declared in the building. Firefighters were immediately on the scene but could not control the fire in SBG2. The whole site has been isolated which impacts all services in SGB1-4. We recommend to activate your Disaster Recovery Plan."

OVHcloud operates 15 datacenters in Europe, with four in Strasbourg and a fifth being built.

The Bas-Rhin report describes an electrical inverter fire that began on the first floor of the five-floor SBG2 structure. The cause of the fire has not been officially declared by OVHcloud and the company did not immediately respond to a request for comment.

### **MORE CONTEXT**

[Talk about a Blue Monday: OVH outlines recovery plan as French data centres smoulder](#)

[OVH rises to Europe data sovereignty challenge \(and AWS\) with tape-as-a-service](#)

[OVH drops IPO target against figure mooted a month ago](#)

[OVHcloud to share its OpenStack automation for use in on-prem clouds](#)

JDN describes how arriving firefighters were met with "electric arcs of more than one meter around the exterior door of the energy room" where the fire is believed to have originated. The report, as algorithmically translated says, "The technicians of ES (Electricité de Strasbourg) met difficulties in cutting off the electricity in the room." ES personnel arrived on-scene about 0120 and didn't manage to cut the power until about 0329.

The report describes the firefighter group leader stating that the temperature in the ground floor room measured 400 degrees Celsius using a thermal camera.

Over 140 customers have [filed a class action lawsuit](#) against the company seeking damages for losses arising from the fire. According to the law firm handling the complaint, Ziegler & Associates, numerous French government websites were affected by the fire, including data.gouv.fr, the National Education website, the Center Pompidou website and Meteosky. The law firm [claims](#) many customers lost their data as a result of the fire and did not understand the need to pay for additional backups. ®

# Reputacinė krizė

- Vieno ;angelio principu dirbantis į ryšius su visuomene skyrius
- Ryšių su visuomene planas kibernetinio saugumo klausimais reputacijai susigrąžinti
- Bendravimas su bendruomene ir klientais

# Atsarginės kopijos.Backups.Backups

- Atsarginės kopijos vietoje
- Atsarginės kopijos ne darbo vietoje
- Duomenų atsarginių kopijų tikrinimas
- Duomenų atkūrimas iš faktinės atsarginės kopijos patikrinimo
- Antriniai serveriai, jei duomenų atkūrimas užtruks daugiau nei 48 valandas

# Kibernetinio saugumo brandos vertinimas

- Kasmetinis nuolatinis kibernetinio saugumo brandos vertinimas
- Informacijos saugumo valdymo sistemų sertifikavimas pagal ISO 27001
- Darbuotojų socialinės inžinerijos ir "Phishing" testai
- Kiekvieno darbuotojo mokymai internetu ir neprisijungus prie interneto įdarbinimo metu, o vėliau - atnaujinimai ir testai
- Kibernetinio saugumo temos mėnesiniuose naujienlaiškiuose darbuotojams ir klientams

# Klausimai ir atsakymai

- Klausimai, pagrįsti pateikta medžiaga
- Jūsų pasakojimai ir galimi įsilaužimo pasekmių sprendimo būdai
- Nestandartiniai įsilaužimų prevencijos būdai
- Temos, kurias praleidome
- Kiti klausimai