ZERO TRUST: kuo pasitikėsime?

Nasdaq Patirtis

Nasdaq | REWRITE TOMORROW

Kaip viskas prasidėjo?

Nasdaq

Nasdaq Hacked

- 2011 metais pasirodė informacija, kad į Nasdaq sistemas JAV buvo įsilaužta;
- Tikėtina, kad kenksmingas kodas buvo patalpintas dar 2010.

BUSINESS INSIDER

TECH | FINANCE | POLITICS | STRATEGY | LIFE | ALL

NASDAQ HACKED

Pascal-Emmanuel Gobry Feb. 5, 2011, 6:12 AM

Hackers have repeatedly broken into Nasdaq's computer systems, the WSJ reports. The trading platform, which executes trades, wasn't compromised, but it's unclear what other systems were.

Apparently the hackers didn't tamper with anything, but it's also unclear whether all holes are plugged, so who knows. Some of the breaches can be traced to Russia, but that doesn't mean the hackers were Russian -- they could simply be using Russian computers as proxies.

Federal investigators, including the Secret Service and the FBI are on the case.

Kelio pradžia

- Sustiprintas InfoSec departamentas:
  - Informacinės saugos strategijos ir politikos valdymo skyrius;
  - InfoSec engineering‘o skyrius;
  - Aplikacijų saugos skyrius (AppSec);
  - Saugos operacijų (stebėjimo ir reagavimo) skyrius (GSOC);
  - Ugniasienių valdymo skyrius;
  - Atitikties skyrius (compliance);
  - Projektų valdymo grupė;

  Ir…
  - IT/kibernetinės saugos auditoriai.

Senasis modelis vs Zero Trust

- Senasis/Tradicinis IT architektūros modelis

https://trakaimuziejus.lt/traku-pilys-kovose-su-kryziuociais

Zero Trust ir Nasdaq

Kontrolės priemonės:

- Informacinės saugos specialistų įtraukimas į procesus;
- Saugi architektūra - kompiuterinių tinklų segmentacija;
- 2FA autentifikacija;
- Administratoriaus teisių valdymas naudojant dedikuotus saugos sprendimus;
- Pilnas pažeidžiamumų skenavimas ir šalinimas;
- Aplikacijų stebėjimas ir kontrolė;
- Apsauga nuo kenksmingo kodo;
- Centralizuotas įvykių stebėjimas (SIEM);
- Web aplikacijų ugniasienės su duomenų srauto dešifravimu;
- Projektas „Kibernetinių grėsmių medžioklė“ (Threat Hunting);
- Tinklo prieigos kontrolės sprendimai (NAC);
- Apsauga nuo DDOS atakų.

Iššūkiai su kuriais susiduriame

Problemos, kurias dar sprendžiame

- Saugos sprendimų įdiegimas 100% apimtimi;
- Įsigytų kompanijų integravimas į korporacijos aplinką;
- Programų kūrimo ir testavimo aplinkos (R&D) saugumas;
- Saugumas „debesijoje“;
- Paslaugų tiekėjų saugumas;
- Legacy IT sprendimų saugumas.

Asmeninės įžvalgos

Nasdaq

Svarbus organizacinės kultūros aspektas

Klausimai?

Nasdaq

AČIŪ

Linas Laucius
Linas.Laucius@Nasdaq.com

Nasdaq