Sigurnosne prijetnje na Internetu

Industrijska špijunaža

Luka Slugečić, 13. studenog 2024.

Pregled predavanja

- Definicija i metode industrijske špijunaže
- Primjeri industrijske špijunaže
- Posljedice i prevencija industrijske špijunaže
- Zaključak
- Literatura

Pitanja za ispite

- Koje su ključne karakteristike industrijske špijunaže?
- Kako se razlikuju industrijska špijunaža i konkurentski obavještajni rad?
- Navedi barem pet najčešćih metoda industrijske špijunaže?
- Koje su moguće posljedice industrijske špijunaže za tvrtke?
- Kako se tvrtke mogu zaštititi od industrijske špijunaže?

Motivacija

- Stvarna i trajna prijetnja
- Financijski gubitci -> propast tvrtke
- Gubitci prema procjenama Cybersecurity Ventures u vrijednosti od nekoliko bilijuna dolara godišnje
- Razumijevanje ove prijetnje i poduzimanje odgovarajućih mjera zaštite ključno je za uspjeh i opstanak svake tvrtke, ali i cijele industrije

Što je industrijska špijunaža?

- IE (engl. *Industrial espionage*) ili
  CI (engl. *Competitive Intelligence*)?
- Za definiciju ključni elementi:
  - Metoda – sustavno prikupljanje informacija
  - Namjera – stjecanje konkurentske prednosti
  - Akter – pojedinac ili organizacija
  - Priroda – (ne)zakonito i (ne)etički

Što je industrijska špijunaža?

- Nezakonita i neetička aktivnost prikupljanja osjetljivih informacija bez dopuštenja vlasnika, s ciljem stjecanja konkurentske prednosti ili prodaje informacija zainteresiranim pojedincima i/ili grupama.

Što je konkurentski obavještajni rad?

- Legalna i etička praksa prikupljanja i analize informacija o konkurenciji i tržištu.
- Koristi javno dostupne informacije kako bi pomogla tvrtkama da donesu bolje poslovne odluke.

Metode industrijske špijunaže?

- „Tradicionalne” metode:
  - Korištenje „*insajdera”* (upućena osoba) – **85%** slučajeva špijunaže, uključuje bivše ili sadašnje zaposlenike, koruptivne prakse i infiltraciju agenata
  - Društveno inženjerstvo
  - Pretraživanje smeća (engl. *dumpster diving*)
  - Angažiranje privatnih detektiva

Metode industrijske špijunaže?

- Moderne metode:
  - Hakiranje
  - Zloćudni kod - *spyware*
  - Phishing – slanje lažnih e-poruka ili stvaranje lažnih web stranica
  - Ilegalno nadziranje – prisluškivanje, tajno snimanje, ozbiljno kršenje privatnosti
  - Krađa prijenosnih računala
  - Reverzno inženjerstvo

Primjeri industrijske špijunaže

- Procter & Gamble vs. Unilever
  - 2001. godina, 10 milijuna dolara
  - Dumpster diving
- Erricson
  - 2002. godina, vojna industrija, diplomatski incident s Rusijom
  - Insajder
- Uber vs. Waymo
  - 2018. godina, 245 milijuna dolara
  - Insjader

Prijetnja kineske vlade

- Ekonomska špijunaža – glavni akter je državna vlast i njeni interesi
- Primjeri:
  - *Thousand talents program* – korištenje kineske emigracije za špijunažu
  - Huawei – posljednjih godina brojne optužbe, između ostalog i krađa intelektualnog vlasništva
  - General Electric – 2023. osuđen inženjer kineskog podrijetla zbog krađe osjetljivih podataka, koristio je steganografiju – osjetljive podatke prikrio u fotografiji

Problemi

- Poteškoće u dokazivanju
  - Fakro vs. Velux
    - 2006. – 2018. godine, tužba odbačena
    - Dugoročne financijske i reputacijske posljedice
- Nespremnost žrtava da prijave incidente
  - Negativni publicitet

Posljedice

- Financijski gubitci
- Gubitak konkurentske prednosti
- Gubitak ugleda
- Gubitak povjerenja klijenata

Prevencija industrijske špijunaže: Tehničke mjere

- Zaštita podataka – šifriranje, sigurnosne kopije, sigurnosni protokoli za prijenos podataka
- Sigurnosni sustavi – vatrozid, antivirus, sustav za detekciju upada (IDS)
- Nadzor pristupa – fizički pristup i pristup putem računalnih sustava

Prevencija industrijske špijunaže: Ljudski faktori

- Edukacija zaposlenika – prepoznavanje sumnjivih aktivnosti
- Podizanje svijesti – prijavljivanje incidenata s jasnim procedurama
- Sigurnosne politike – procedure za rukovanje informacijama, pristup sustavima i korištenje tehnologije
- Provjera zaposlenika – prije zapošljavanja provjera životopisa, preporuka i kaznene evidencije

Zaključak

- Ozbiljna prijetnja poslovanju
- Globalna i stalno prisutna opasnost
- Važno je razlikovati zakoniti konkurentski obavještajni rad od nezakonitih praksi špijunaže
- Prevencija je ključna

Literatura

- Hou, Tie, and Victoria Wang. "Industrial espionage–A systematic literature review (SLR)." *computers & security* 98 (2020): 102019.
- Button, Mark. "Economic and industrial espionage." *Security Journal* 33 (2020): 1-5.
- Solberg Søilen, Klaus. "Economic and industrial espionage at the start of the 21st century–Status quaestionis." *Journal of Intelligence Studies in Business* 6.3 (2016): 51-64.
- Crane, Andrew. "In the company of spies: When competitive intelligence gathering becomes industrial espionage." Business Horizons 48.3 (2005): 233-240.

Literatura

- Tzenios, Nikolaos. Corporate Espionage and the Impact of the Chinese Government, Companies, and Individuals in Increasing Corporate Espionage. Apollos University, 2023.
- Industrial espionage: How China sneaks out America's technology secret, BBC, pristupljeno 7.11. 2024., poveznica: https://www.bbc.com/news/world-asia-china-64206950
- The China Threat, FBI, pristupljeno 7.11.2024., poveznica: https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans
- What we learned in the Waymo v. Uber case, CNN Business, pristupljeno 7.11.2024., poveznica: https://money.cnn.com/2018/02/10/technology/waymo-uber-what-we-learned/index.html

Dodatna literatura

- Holmström, Lauri. "Industrial espionage and corporate security: the Ericsson case.” Reports of the Police Collage of Finland 87/(2010).
- Dalal, Mukesh, and Mamta Juneja. "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide." Multimedia Tools and Applications 80.4 (2021): 5723-5771.

Hvala!