Zdravje. Znanost. Vedno tu.
Health. Science. Always here.

univerzitetni
klinični center ljubljana
University Medical Centre Ljubljana

KIBERNETSKA VARNOST V JZZ ZA VARNEJŠI JUTRI – INVESTICIJA ALI STROŠEK?

Andrej Dočinski, dipl. var.,

vodja Službe za korporativno varnost UKC Ljubljana

„I am convinced that there are only two types of companies: those that have been hacked and those that will be.“

„ And even they are converging into one category: companies that have been hacked and will be hacked again.“

Robert S. Mueller – direktor FBI, 2012

Avtor:
I. H.

Ponedeljek,
15. 1. 2024,
14.08

1 leto, 9 mesecev

6,45

Natisni članek

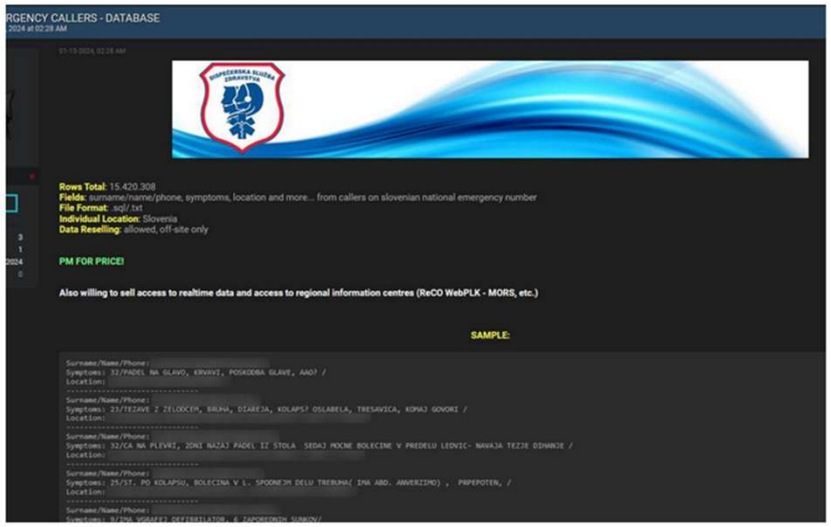
hekerji

Košarkarski škandal: je bil Rus sodelavec zloglasnih kriminalcev?

Ukrajina vdrla v eno od najpomembnejših podjetij v Rusiji in...

Bo Ukrajina kmalu dobila novo vrsto vojakov?

Nov napad na Slovenijo: vdora ni bilo, kako so se podatki torej znašli na spletu?



Oglas za prodajo baze podatkov

Foto: Siol.net

Na temnem spletu so neznani hekerji prodajali bazo podatkov, ki naj bi vsebovala posnetke telefonskih klicev na številko 112. Hekerji so tudi trdili, da imajo še vedno odprt neposreden dostop do baze. Na uradu za informacijsko varnost so za Siol.net potrdili, da so bili obveščeni o pojavu osebnih podatkov za zdravstveno vsebino na temnem spletu, ne pa o kibernetskem incidentu.

Kot so nam pozno popoldne sporočili z urada za informacijsko varnost, storitev 112 pripada URSZR, podatke o uporabi nujne medicinske pomoči pa vnaša Dispečerska služba zdravstva, ki jo upravlja UKC Ljubljana. Kot so sporočili, je zadevo prevzela služba za korporativno varnost UKC, ki bo obvestila policijo in urad za informacijsko varnost. "Izvajajo se vsi ukrepi, predvideni v primeru takšnih dogodkov," so zagotovili na UKC Ljubljana.

UKC Ljubljana je kot prvi JZZ v Republiki Sloveniji

kibernetsko varnost opredelili kot

temeljni element korporativnega varovanja organizacije

kot celote in ne zgolj kot tehnično nalogo

Področja za informatiko.

1. Uvod

- V zadnjih letih je področje zdravstva napredovalo na številnih področjih, še največ na področju digitalizacije.
- Zdravstvene organizacije, zlasti javni zdravstveni zavodi (JZZ), so postale tarča vse pogostejših in vedno bolj sofisticiranih kibernetskih napadov.
- Kibernetski napadi ogoržajo ne samo podatke ampak tudi zaupanje, varnost pacientov in neprekinjeno oskrbo.

2. Kibernetska varnost kot širši okvir varovanja

- **Korporativna varnost** je sistem ukrepov, ki vključujejo pravne, organizacijske, kadrovske in tehnične vidike varovanja organizacije.
- **Kibernetsko varnost** lahko definiramo kot skupek ukrepov, praks in procesov, ki ščitijo informacijske sisteme, omrežja, podatke in digitalne informacije pred nepooblaščenim dostopom, zlorabo, poškodbami ali motnjami.
- Vloga Enote za kibernetsko varnost SKV UKCL je strateško usmerjati zgoraj naštete aktivnosti v sodelovanju s Področjem za informatiko in drugimi organizacijskimi enotami ter službami znotraj UKCL.

3. Aktualne grožnje in incidenti v zdravstvu

- Zdravstveni sektor žal predstavlja enega bolj zaželenih ciljev kibernetskih napadov zaradi visoko »dragocenih« podatkov pacientov.
- Aktualne grožnje in incidenti v zdravstvu:
  - **Ransomware napadi:** napadalci zaklenejo dostop do sistemov ali podatkov in zahtevajo odkupnino za odklep.
  - **Kraja in zloraba zdravstvenih podatkov:** zajema krajo občutljivih osebnih podatkov pacientov, kar vodi do zlorabe identitet, nepooblaščenega dostopa ali razkritja zaupnih informacij.
  - **Napadi na medicinske in IoT naprave:** naprave lahko dostopne preko omrežij in niso vedno dovolj zaščitene.
  - **Notranje grožnje in socialni inženiring:** predstavljajo nepravilno uporabo informacijskih sistemov, neozaveščenost zaposlenih ter notranje zlorabe.
  - **Motnje delovanja IT infrastrukture:** so napadi, ki povzročijo izpad delovanja informacijskih sistemov (npr. DoS napadi).

4. Stroški kibernetskih incidentov

- Kakšna je resnična cena varstva?
- Stroški kibernetskih incidentov v zdravstvu:
  - **Neposredni finančni stroški,** ki vključujejo stroške za obnovo informacijskih sistemov, forenzične preiskave, plačilo odkupnin…
  - **Operativne motnje in prekinitve storitev IT sistemov,** ki povzročijo zamude ali popolne prekinitve zdravstvenih storitev, kar lahko ogrozi zdravje in življenje pacientov.
  - **Reputacijska škoda in izguba zaupanja pacientov in javnosti,** kar se lahko odrazi v zmanjšanem številu pacientov in višjih stroških za obnovo ugleda.
  - **Pravni in regulativni stroški,** ki lahko ob neupoštevanju zahtev in standardov varstva podatkov povzročijo visoke kazni s strani nadzornih organov, zahteve za odškodnine ter pravne postopke.
  - **Posredni stroški,** ki vključujejo dodatne človeške vire, povečano administracijo, stroške povečane varnosti po incidentu ter izgubo produktivnosti zaposlenih zaradi odzivanja na incident.

5. Kibernetska varnost kot trajnostna investicija

- Z vidika strategije je smiselno razumeti kibernetsko varnost kot investicijo, ki povečuje odpornost in zagotavlja neprekinjeno poslovanje.
- Investicije morajo zajemati:
  - Tehnološke rešitve (firewall, nadzor omrežja, varnostne kopije),
  - Kadrovske vire (zaposlovanje v SKV, izobraževanja),
  - Organizacijske procese (politike, postopki, odzivnost na incidente),
  - Sodelovanje in izmenjavo informacij z drugimi ustanovami in državnimi organi.

6. Model upravljanja kibernetske varnosti v UKCL

- Model upravljanja kibernetske varnosti v UKCL temelji na celostnem, interdisciplinarnem pristopu, ki vključuje kombinacijo organizacijskih, tehničnih in kadrovskih ukrepov, usklajenih z vodstvom in SKV. Ključni elementi takšnega modela so:
  - Vzpostavitev jasnih odgovornosti med SKV, Področjem za informatiko in ostalimi organizacijskimi enotami znotraj UKCL.
  - Vzpostavitev centraliziranega nadzora in odziv na varnostne incidente- Integrirani Security Operating Center (iSOC) - združuje kibernetski nadzor (SIEM, XDR), video nadzor, fizično varovanje in analitiko v realnem času. Tak center omogoča celovit pregled nad varnostnim stanjem, hitro prepoznavanje incidentov in usklajeno krizno upravljanje.
  - Redne ocene tveganj ranljivosti informacijskih sistemov in simulacije.
  - Izobraževanje in zavedanje zaposlenih.
  - Krizno načrtovanje in hitri odziv - zajema pripravo jasnih kriznih načrtov z določenimi postopki in vlogami za hitro omejitev škode in vzpostavitev delovanja sistema po incidentu.

7. Zaključek

- Kibernetska varnost ni strošek, ampak predvsem strateška in trajnostna investicija v varnost, zanesljivost ter dolgoročno odpornost javnega zdravstvenega sistema.
- Stroški odprave posledic kibernetskih incidentov so znatno višji od stroškov preventivnih ukrepov in investicij v varnostne tehnologije, zaposlene ter usposabljanja.
- Kibernetsko varnost razumemo kot pomembno investicijo, ki ne prinaša le zaščite pred napadi, temveč omogoča tudi varno uvajanje inovacij, digitalizacijo in zagotavljanje neprekinjene zdravstvene oskrbe.
- Investicija v kibernetsko varnost je veliko bolj vzdržna in ekonomična kot stroški odpravljanja incidentov, zato mora biti strateško umeščena kot prioritetna naloga korporativnega upravljanja vsakega JZZ.

HVALA!