Kibernetski incidenti in odgovornost poslovodstva v luči sodne prakse

Jure Planinšek

NIL
Part of Conscia

Varnostni incidenti kot posledica phishinga

Kaj večina misli, da je phishing?

Trendi Phishinga v 2026: Kaj postaja phishing?

- **AI-podprti socialni inženiring:** napadalci uporabljajo generativno AI za prepričljiva besedila brez slovničnih napak, *smishing* in *vishing*, hibridni napadi

- ***Shadow AI*:** malomarno ravnanje uporabnikov s podatki (vnašanje poslovnih skrivnosti / osebnih podatkov v javna gen AI orodja)

- **Zlorabe identitet:** zloraba QR kod, MFA bypass – napadi ne ciljajo le gesel, temveč prijavne žetone in aktivne seje

"Človek ostaja najšibkejši člen: Napad na zaupanje"

Zlonamerni *insider ali neskrbni zaposleni?*

Kategorija	**Ključni razlog**	**Učinek**	Možni ukrepi
(Ne)skrbni zaposleni	Shadow AI, napake pri delu na daljavo, phishing	~55 % notranjih incidentov	Izobraževanje, postopki, nadzor, kultura, tehnični ukrepi
Zlonamerni zaposleni	Finančna korist, zloraba pravic dostopa	Najvišji strošek	Tehnični ukrepi, (procesne) kontrole in nadzor
Zunanji izvajalci	Prekomerni dostopi, kompromitira na omrežja	~15–25 % vseh notranjih groženj	Pogodbene zaveze, tehnične kontrole in ukrepi

Zaposleni ali poslovodstvo (podjetje)?

REPUBLIKA SLOVENIJA
VIŠJE DELOVNO IN SOCIALNO SODIŠČE

VDSS Sodba Pdp 529/2024

Sodišče: Višje delovno in socialno sodišče
Oddelek: Oddelek za individualne in kolektivne delovne spore
ECLI: ECLI:SI:VDSS:2025:PDP.529.2024
Evidenčna številka: VDS00083784
Datum odločbe: 08.01.2025
Senat: dr. Martina Šetinc Tekavc (preds.), Mojca Dubravica (poroč.), Jelka Zorman Bogunovič
Področje: DELOVNO PRAVO - ODŠKODNINSKO PRAVO
Institut: odškodninska odgovornost delavca - huda malomarnost delavca

Jedro

Tožnica ni uspela dokazati hude malomarnosti toženke, torej zanemarjanje tiste pazljivosti in skrbi, ki se pričakuje od vsakega povprečno skrbnega človeka, v konkretnem primeru od povprečno skrbnega računovodje.

Izrek

I. Pritožba se zavrne in se potrdi izpodbijana sodba sodišča prve stopnje.

II. Tožeča stranka je dolžna toženi stranki povrniti stroške odgovora na pritožbo v višini 1.023,89 EUR v roku 15 dni, svoje pritožbene stroške pa krije sama.

Obrazložitev

1. Sodišče prve stopnje je zavrnilo tožbeni zahtevek, da je dolžna toženka tožnici plačati 90.000,00 EUR z zakonskimi zamudnimi obrestmi od 31. 3. 2021 dalje ter ji povrniti vse priglašene stroške skupaj z zakonskimi zamudnimi obrestmi (točka I izreka). Tožnici je naložilo povrnitev stroškov postopka toženke v višini 3.147,49 EUR skupaj z zakonskimi zamudnimi obrestmi od poteka izpolnitvenega roka dalje do plačila (točka II izreka) ter kot zavezanko za plačilo sodne takse določilo tožnico (točka III izreka).

2. Zoper tako prvostopno odločitev se po svoji pooblaščenki iz vseh pritožbenih razlogov pravočasno pritožuje tožnica s pritožbenim predlogom na spremembo izpodbijane sodbe v smeri ugoditve tožbenemu zahtevku v celoti in naložitve toženki, da tožnici povrne pravdne stroške, podrejeno pa predlaga njeno razveljavitev in vrnitev zadeve sodišču prve stopnje v novo sojenje. Po prepričanju tožnice je sodišče prve stopnje zmotno uporabilo materialno pravo, ko je pri odgovoru na bistveno vprašanje, ali je toženka ravnala v nasprotju s skrbnostjo, ki jo gre pričakovati od vsakega povprečno skrbnega človeka oziroma v predmetni zadevi povprečno skrbnega računovodje, napačno zaključilo, da toženki ni mogoče očitati hude malomarnosti. Tak zaključek je sprejelo že zgolj na podlagi dejstva, da so bila sporočila neznanega storilca kreirana na ime A. A. in poslana v njegovi odsotnosti ter dejstva, da je A. A. prejete račune vnašal po datumu zapadlosti. Po prepričanju tožnice je zaključek sodišča prve stopnje nelogičen in neživljenjski upoštevaje dejstvo, da je toženka na račun neznanih storilcev nakazala kar 100.100,00 EUR, nakazila pa so bila izvedena v razmaku štirih dni. Tudi toženka sama je implicitno potrdila, da so bila elektronska sporočila nenavadna, saj je po prejemu prvega elektronskega sporočila poklicala A. A. Po prepričanju tožnice so trditve toženke prilagojene potrebam postopka, saj bi domnevno neuspešen klic izkazal njeno skrbnost. Iz dejstva, da se je toženki zdelo potrebno poskusiti priklicati A. A., pa izhaja, da je prejeto sporočilo pri njej vzbudilo dvom v njegovo avtentičnost oziroma resničnost kakor tudi, da je očitno vedela, da bi morala za izvedbo nakazil dobiti ustno odobritev A. A., vendar je kljub temu plačilo izvedla brez teh potrebnih korakov. Sodišče prve stopnje je neutemeljeno verjelo toženki, da posebnih navodil ni prejela, čeprav zgolj dejstvo, da navodila niso bila pisna in z njimi ni bil seznanjen B. B. (zakoniti zastopnik tožnice), ne more predstavljati dokaza za njihov neobstoj. Iz izpovedbe A. A. izhaja, da je bil postopek izvedbe plačil za C. jasen: vedno zgolj na podlagi fizične listine ter ob ustni potrditvi A. A. Iz obrazložitve izpodbijane sodbe ni mogoče razbrati, kaj naj bi toženka utemeljeno štela za podlago nakazila (naložba ali plačilo računov vodičev za potovanje). Tožnica se tudi ne strinja s prvostopnim stališčem, da toženki ni mogoče šteti v breme, da je šlo za nove, tuje transakcijske račune. Drži sicer, da je toženka pogosto opravljala plačila v tujino, vendar zgolj s povezanimi družbami ali s podlago, ki je bila toženki jasno poznana. Kot že v postopku na prvi stopnji izpostavlja, da so bila elektronska sporočila pripravljena v polomljeni slovenščini, posledično bi morala toženka zaradi dolgoletnega sodelovanja z A. A. odstop od običajnega zaznati. Z drugačnim zaključkom sodišča prve stopnje se ne strinja, prav tako tudi ne z absurdnim stališčem, da odsotnost odpovedi oziroma uvedbe delovnopravnega postopka nakazuje na to, da tožnica toženkinega ravnanja ni štela za hudo malomarnost. Odsotnosti uvedbe postopka odpovedi pogodbe o zaposlitvi nikakor ne gre šteti za tiho odobravanje protipravnih ravnanj toženke. Tožnica predlaga kot uvodoma navedeno in priglaša pritožbene stroške.

V škotskem primeru Peebles Media je podjetje neuspešno tožilo zaposleno za ~100.000 £ izgube v BEC-prevari, ker je ni nikoli usposobilo za prepoznavanje prevar.

- ➔ Odgovornost za kibernetsko varnost primarno nosi podjetje, ne posameznik. Računovodkinja, ki je pod vplivom lažnih e-sporočil (CEO-fraud) nakazala 90.000 €, ni bila odškodninsko odgovorna.
- ➔ Zahtevek do delavca je po 147. členu OZ in 177. členu ZDR-1 mogoč le ob dokazanem naklepu ali hudi malomarnosti (skrajna nepazljivost povprečno skrbnega delavca na tem delovnem mestu).
- ➔ Prag hude malomarnosti je zelo visok: brez jasnih, vnaprej sprejetih pravil in kontrol je skoraj nedosegljiv.
- ➔ Dokazno breme je na strani organizacije

👩‍💻 Pravne posledice za zaposlene - povzetek

Posledica	Pogoj	Pravna podlaga
Odškodninska odgovornost	Le pri naklepu ali hudi malomarnosti; dokazno breme na delodajalcu	177. čl. ZDR-1, 147. čl. OZ
Disciplinski ukrep / odpoved pogodbe o zaposlitvi	Kršitev internih pravil (dokazljivo komuniciranih)	83., 89., 110. čl. ZDR-1
Kazenska odgovornost	Le pri naklepnih dejanjih (sabotaža, zlonamerni insider)	237. čl. KZ-1
Brez posledic	Če podjetje ni imelo jasnih postopkov, usposabljanj in nadzora	VDSS Pdp 529/2024

👨‍💼 Odgovornost poslovodstva (direktorjev osebno)

Posledica	Kaj to pomeni v praksi	Pravna podlaga
Osebna odškodninska odgovornost	Družba (ali v stečaju upniki) lahko od direktorja osebno zahteva povrnitev škode, ki jo je podjetje utrpelo zaradi incidenta. Direktor mora dokazati, da je ravnal pravilno.	263. čl. ZGD-1
Osebna odgovornost za kibernetsko varnost	Direktor je po zakonu osebno odgovoren, da podjetje upravlja kibernetska tveganja. Ne more se izgovarjati, da »za to skrbi IT« ali da »ni vedel«. Mora se tudi redno usposabljati (vsaj vsake 4 leta).	ZInfV-1 (20.–22. čl.)
Kazenska odgovornost	V skrajnih primerih, npr. namerno prikrivanje incidenta ali zavestna opustitev varnostnih ukrepov, kazenska odgovornost direktorja ni izključena. V praksi je to redko, a možno.	KZ-1
Razrešitev (izguba položaja)	Nadzorni svet ali lastniki lahko direktorja razrešijo in zamenjajo, če ocenijo, da ni ustrezno upravljal kibernetskih tveganj.	ZGD-1

🏢 Odgovornost organizacije (družbe)

Posledica	Kaj to pomeni v praksi	Pravna podlaga
Globe za kršitev kibernetske varnosti	Globa do 10 mio EUR ali 2 % letnega prometa (za ključna podjetja) oziroma do 7 mio EUR ali 1,4 % (za pomembna podjetja).	ZInfV-1
Globe za kršitev varstva osebnih podatkov	Če incident vključuje osebne podatke, lahko Informacijski pooblaščenec izreče globo do 20 mio EUR ali 4 % letnega prometa.	GDPR, ZVOP-2
Pogodbene kazni in odškodnine	Stranke, dobavitelji ali posamezniki lahko zahtevajo plačilo škode (npr. kršitev pogodbe, zamude, izpad storitev).	OZ, pogodbe
Izguba licenc ali dovoljenj	V reguliranih panogah (bančništvo, zavarovalništvo) lahko regulator podjetju odvzame dovoljenje za poslovanje.	Sektorska zakonodaja
Izguba ugleda in strank	Incident lahko povzroči izgubo zaupanja strank, partnerjev in javnosti: škoda, ki je pogosto večja od glob.	/

Povzetek

🏢 Podjetje plača globe in odškodnine.
Najhujši incidenti: stečaji.

👩‍💼 Direktor odgovarja osebno, s svojim premoženjem in položajem.

👩‍💻 Zaposleni odgovarja, če mu podjetje dokaže naklep ali hudo malomarnost in če je prej imelo jasna pravila.

Phishing - ZInfV-1 in sodna praksa

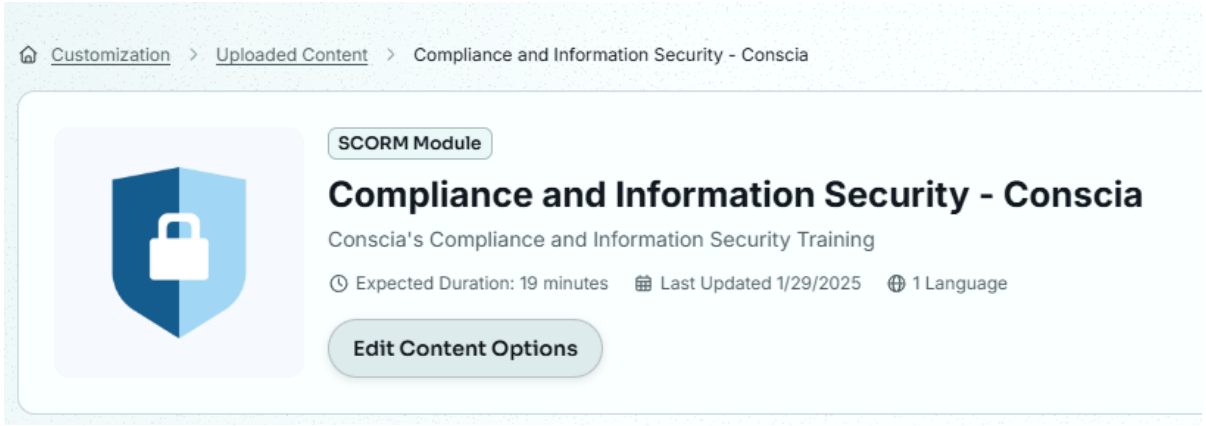
# ukrepa	Ukrep za obvladovanje tveganja po 22. členu	Zakaj je relevanten za phishing
3	Kibernetska higiena in redno usposabljanje	Zaposleni morajo znati prepoznati phishing, usposabljanja morajo biti redna, ne enkratna
4	Nadzor dostopov in upravljanje pooblastil	Načelo najmanjših privilegijev → tudi če phishing uspe, napadalec dobi manj (npr. segmentiranje omrežij)
15	Večfaktorska avtentikacija (MFA)	Tudi, če napadalec ukrade geslo preko phishinga, brez drugega faktorja ne pride v sistem; izzivi naprednih napadov (token, identity)
14	Zaščita pred zlonamerno kodo	EDR/antimalware zaustavi priponke in zlonamerne povezave iz phishing sporočil
6	Dnevniški zapisi (hramba min. 6 mesecev, 24. čl.)	Brez logov ne morete ugotoviti, kaj se je zgodilo po uspešnem phishingu
8	Kriptografija in šifriranje	Tudi če napadalec pride do podatkov, so šifrirani podatki zanj neuporabni

“Phishing ni omenjen poimensko, a je zajet skozi najmanj 6 od 17 obveznih ukrepov.”

“Temeljna dolžnost vodstva je zagotavljanje virov in spremljanje izvajanja ukrepov.”

Najboljše prakse

Kibernetska higiena in redno usposabljanje



Najboljše prakse

Nadzor dostopov in upravljanje pooblastil

🔑 **Upravljanje privilegiranih dostopov (PAM)**

🛡️ **Večfaktorska avtentikacija (MFA)**

👁️ **Pregled in revizija dostopov (Access Review)**

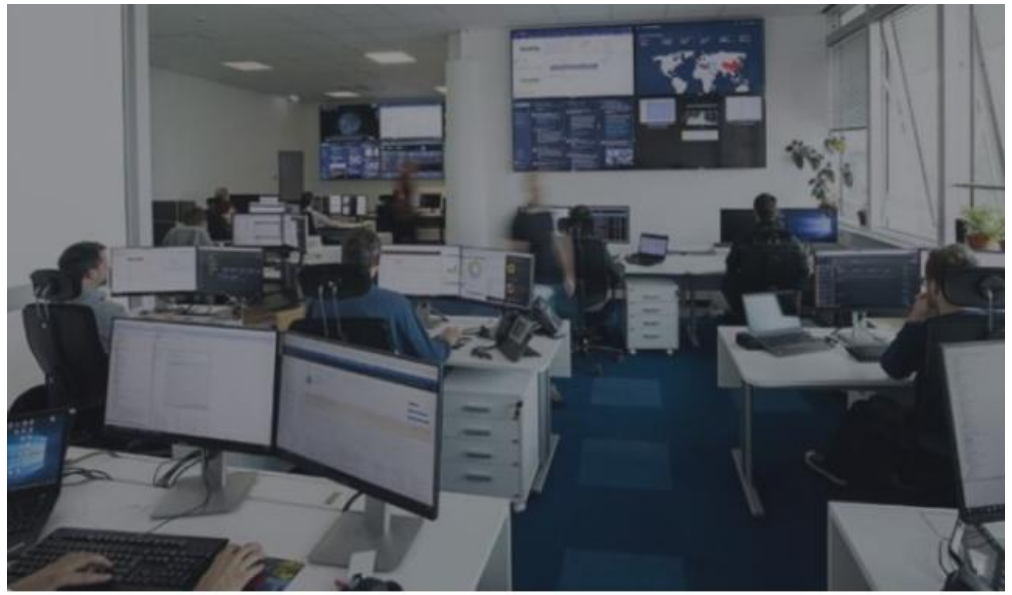
🔄 **Upravljanje življenjskega cikla identitet**

🧱 **Segmentacija in načelo najmanjših pravic**

Najboljše prakse

24/7 monitoring

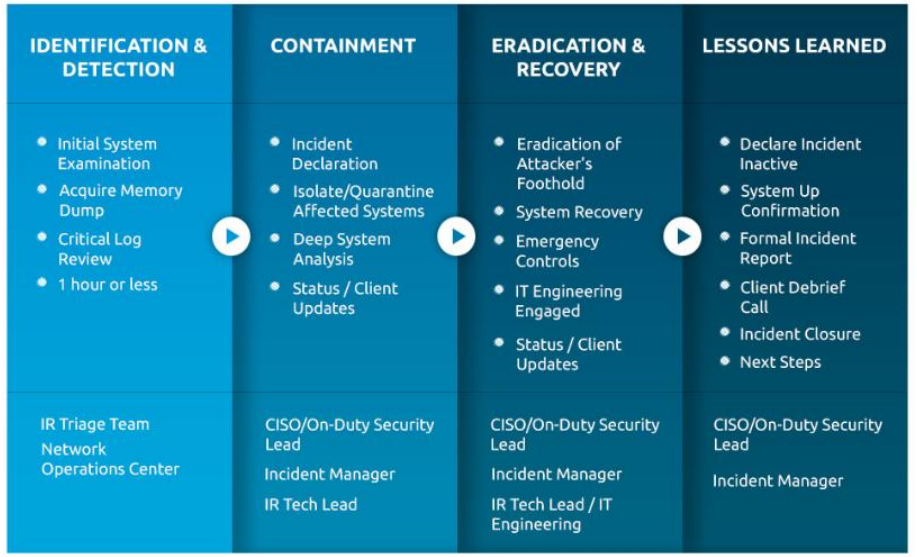
Red Teaming



“Prijava incidenta brez stigme, ker je to del kulture podjetja.”

Najboljše prakse

- Postopki in procesi

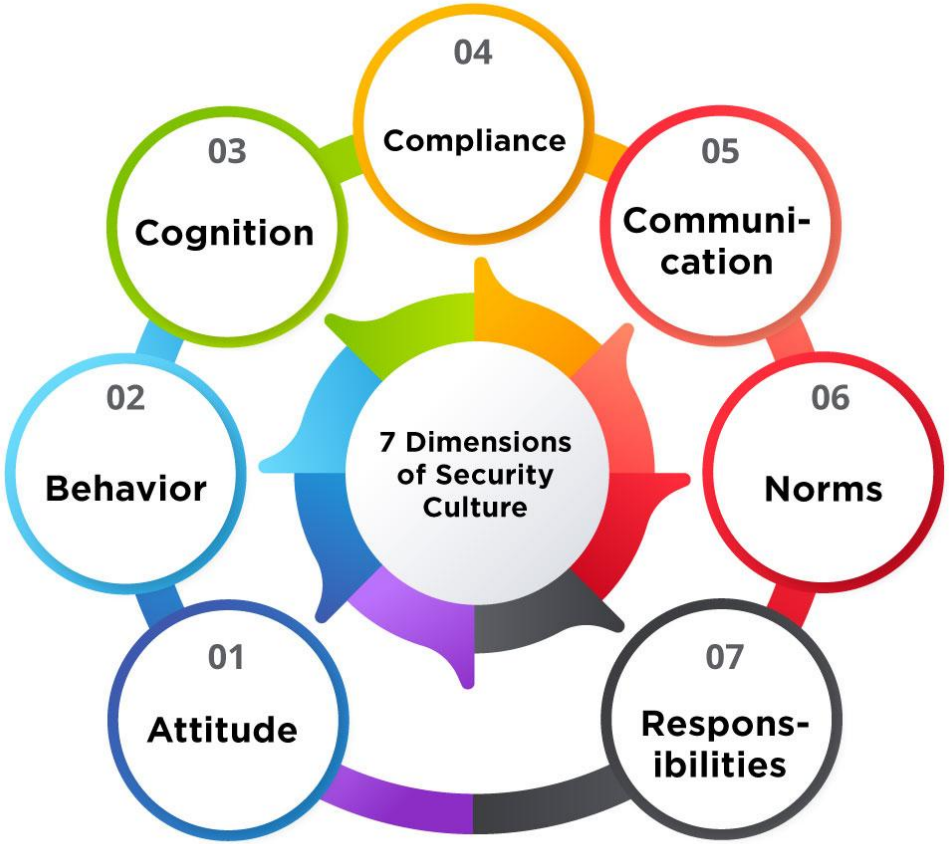


Najboljše prakse

- Kultura

“Če zaposleni klikne na okuženo povezavo, ker ni bil izobražen ali ker se boji prijaviti napako, je to sistemski poraz vodstva, ne le napaka posameznika.

Odgovornost vodstva je postaviti jasna pravila, zagotoviti vire in redno preverjati, ali ukrepi delujejo v praksi. Ustvariti je treba kulturo, kjer je varnost del vsakodnevnih procesov, in kjer je prijava incidenta pričakovana, podprta in dokumentirano obravnavana.”



Hvala za pozornost!

Jure Planinšek
jplaninsek@nil.com

NIL
Part of Conscia