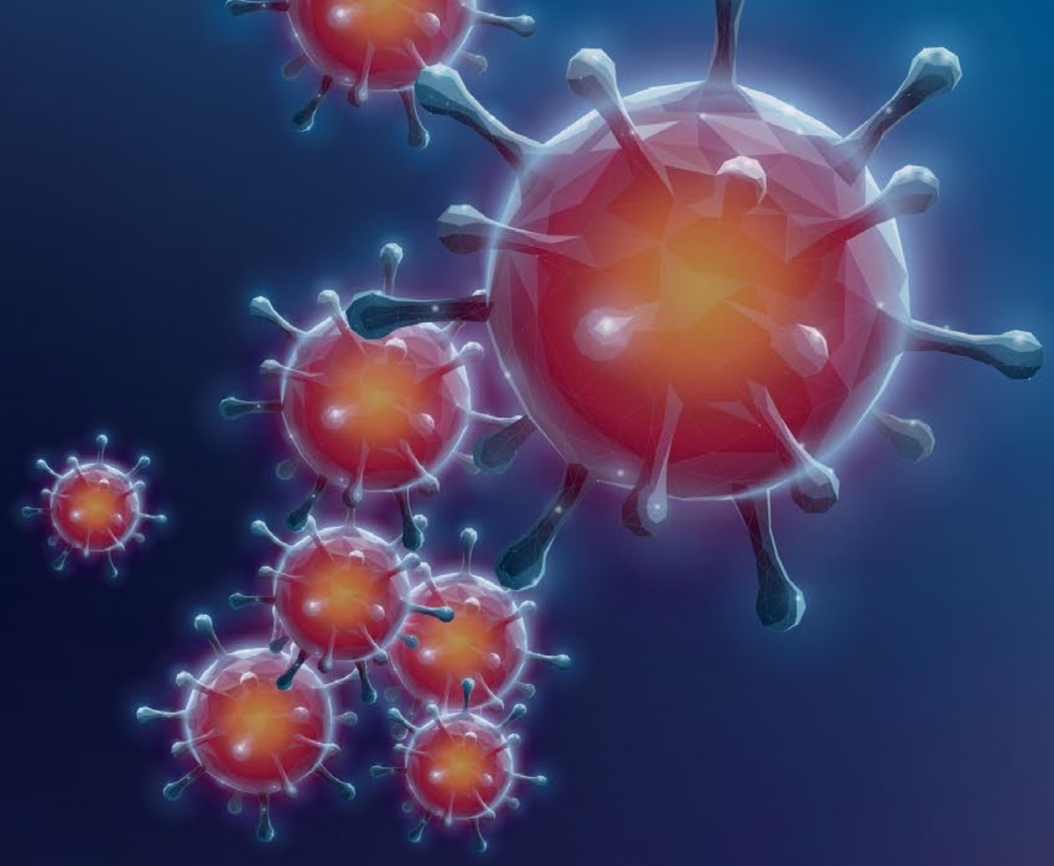
si·cert 25

Varni v pisarni



Samo en napačen klik lahko pomeni neznansko škodo za podjetje. Za varnost podjetja ste odgovorni tudi zaposleni in ker ste nevarnostim pogosto najbolj izpostavljeni ravno vi, smo za vas pripravili nekaj koristnih napotkov.

Previdno pri elektronski pošti!

Elektronska pošta je eden izmed najpogostejših vektorjev kibernetskih napadov, hkrati pa tudi naš glavni, če ne celo edini vir komunikacije v podjetju. Z napadi prek elektronske pošte lahko napadalci pridobijo dostop do računalnika, nam ukradejo gesla, poslovne skrivnosti in druge občutljive podatke, nam zašifrirajo dokumente ter nas izsiljujejo z javno objavo ukradenih podatkov.

Škodljive priponke

Računalniški virusi se najpogosteje širijo prek priponk v okuženih elektronskih sporočilih. Največkrat so to arhivske datoteke vrste zip, včasih pa imajo tudi kakšno drugačno končnico, ki je veliko uporabnikov niti ne prepozna, npr. rar, iso, img ipd. Nevarne so tudi na prvi pogled nenevarne MS Office datoteke, ki za ogled vsebine zahtevajo klik na gumb »Omogoči vsebino«. S tem aktivirate škodljive makre, ki na računalnik namestijo virus. Makre lahko uporabljate samo takrat, ko dokument prejmemo iz zanesljivega vira in veste, zakaj jih potrebujemo (recimo za računovodstvo).

Ključni napotki

Sumljivo je, če e-mail zahteva, da nujno odprete priponko, ker pošiljatelj pričakuje takojšen odgovor. Hkrati pa niste točno prepričani, zakaj ste prejeli ta e-mail, tudi če je vezan na vaše področje dela.

Enako velja za povezave v sporočilih, če niste prepričani, ne klikajte! Tudi tako aktivirate virus, ali pa vam ukradejo geslo, ko e-mail vsebuje povezavo za prenos nekega dokumenta.

V polju Pošiljatelj se navadno izpišeta ime in priimek osebe, s katero komuniciramo, ne pa tudi e-naslov. Zato redno preverjajte, če gre za res pravi e-naslov te osebe!

Sumljivo je vse, kar odstopa od predhodne komunikacije, npr. naenkrat sogovornik napiše stavek ali dva v polomljeni slovenščini in zahteva, da nujno odprete priponko ali pošlje e-mail z drugega naslova.

Vsako spremembo v načinu plačevanja računov (npr. drug bančni račun, neobičajno urgentno plačilo ipd.) preverite preko telefona.

Virus lahko pride tudi v sporočilu, ki vsebuje preteklo komunikacijo (npr., kot da vam nekdo odgovarja na vaše prejšnje sporočilo).

Kraja gesel

Napadalci do naših gesel pridejo na različne načine, najpogostejši pa so:

- prek phishing napada, v katerem napadalcem kar sami sporočimo geslo;
- prek okužbe računalnika z virusom, ki ukrade shranjena in vpisana gesla;
- prek vdorov v baze uporabnikov spletnih storitev, v katere smo registrirani.

Ravno zato je izjemno pomembno, da za vsako storitev uporabljamo drugo geslo. Če uporabljamo isto geslo za različne storitve, potem lahko napadalci z vdorom zgolj v eno od baz podatkov pridobijo dostop do vseh ostalih storitev, ki jih uporabljate.

Sami lahko ustvarite unikatna gesla z lastnim »algoritmom«, ali pa za varno hrambo uporabljate upravljalnika gesel, npr. 1password, LastPass, KeePass, Keeper, RoboForm. Z njimi lahko generirate unikatna gesla, omogočajo pa vam tudi varno shranjevanje gesel.

2FA

Kadar je mogoče, vklopite 2FA oz. dvofaktorsko avtentikacijo. Dvofaktorska avtentikacija je dodatna zaščita, pri kateri morate ob prijavi poleg gesla vnesti še dodatno kodo, ki jo prejmete v SMS sporočilu, ali pa jo zgenerirate z aplikacijo na pametnem telefonu oz. s posebno napravo za generiranje kod. Na ta način napadalci ne bodo mogli vdreti v vaš račun, tudi če vam uspejo ukrasti geslo.

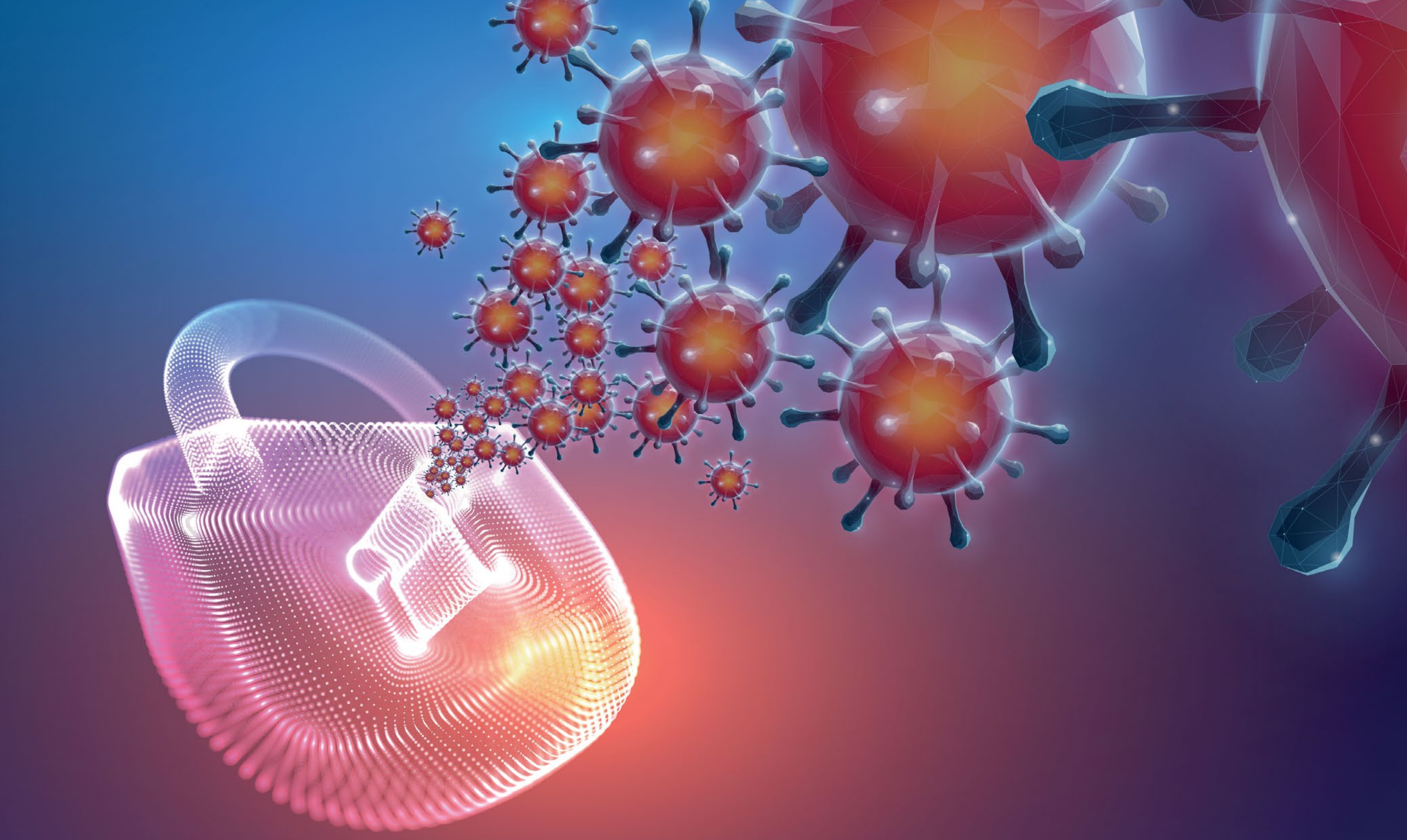
Takoj obvestim odgovorno osebo!

Ko ste v dvomih, se obrnite na odgovorno osebo v vaši organizaciji! Če dobite čuden e-mail, pa ne veste točno, zakaj ste ga prejeli, se vam zdi karkoli sumljivo, raje preverite.

Kontaktirajte vašega informatika, varnostnega inženirja, ali tisto osebo, ki pri vas skrbi za varnost in/ali IT.

Vzemite si 30 minut za informacijsko varnost

Na Nacionalnem odzivnem centru SI-CERT smo zasnovali BREZPLAČNI spletni tečaj za izobraževanje zaposlenih o informacijski varnosti. Tečaj bo od jeseni dalje dostopen na www.varnivpisarni.si.



Kdaj prijaviti incident

OKUŽBA RAČUNALNIKA

izsiljevalski virusi, bančni trojanci, ciljani napadi, agenti za pošiljanje neželene elektronske pošte

Kaj storimo? → **Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do zdaj znanimi grožnjami; svetovanje o ukrepih za sanacijo stanja.**

NAPAD ONEMOGOČANJA

poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja

Kaj storimo? → **Ocena o uporabljenih sredstvih za napad, opredelitev možnih zaščitnih ukrepov, poskus onemogočanja botneta in obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti.**

OPAŽEN VDOR V STREŽNIK

razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij storilca

Kaj storimo? → **Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito.**

IZGUBA GESEL ALI KRAJA OMREŽNE IDENTITETE

zloraba prek phishing napada ali napada okužbe računalnika

Kaj storimo? → **Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in iskanju storilca.**

SUMLJIVA ELEKTRONSKA SPOROČILA

phishing sporočila, ponudbe o hitrem zaslužku ali posojilih

Kaj storimo? → **Odstranjevanje in označevanje lažnih spletnih mest. Prepoznava širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.**

RANLJIVE ALI IZPOSTAVLJENE STORITVE

vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja

Kaj storimo? → **Obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve.**

SPLETNA GOLJUFIJA

lažne spletne trgovine, prevare pri prodaji in nakupih prek spletnih posrednikov, lažna posojila, nigerijske, loterijske in ljubezenske prevare

Kaj storimo? → **Ocena tveganja, odstranjevanje lažne spletne trgovine s spleta, ozaveščanje javnosti**.

si·cert 25