

Kako se obraniti od kibernetičkih napada i zaštititi posao/ugled?

Što vlasnici i direktori moraju odlučiti i učiniti prije incidenta?

Nije pitanje hoće li će se kibernetička ugroza dogoditi, nego kada će se dogoditi i koliku štetu će prouzročiti!



Tehnologija prevedena u poslovne odluke



30+

godina iskustva u poslu,
IT-u i inovacijama

CEO

osnivač i direktor tvrtke
CITUS

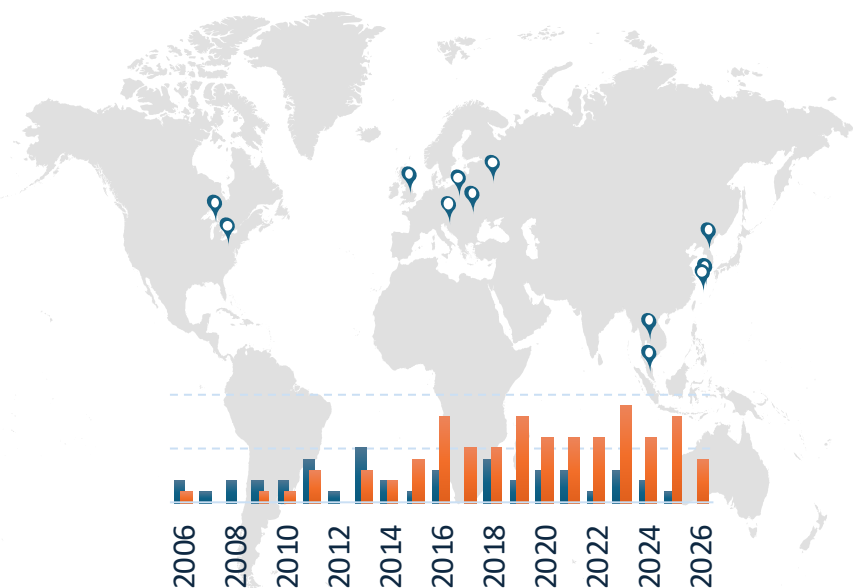
RD+MVP

Microsoft Regional Director i
MVP za Microsoft 365

Poduzetnik • inovator • šest patenata • poslovno i tehničko iskustvo • viši predavač



CITUS spaja strategiju, tehnologiju i provedbu



125

međunarodnih nagrada za
ICT inovacije

6

vlastitih patenata u području
ICT-a

Kibernetička sigurnost • digitalna transformacija • Microsoft 365 i Azure • razvoj i AI

Upravo SADA u ovoj dvorani nalaze se predstavnici tvrtki koje su:

- **Doživjele kibernetički napad i srame se to priznati**
- **Kibernetički napadnute i to još uvijek ne znaju**
- **Upravo sada predmet kibernetičkog napada**



Prijetnja je stvarna, a posljedica je poslovna

1.513

incidenata obradio je
Nacionalni CERT

+35,94%

više prijava nego godinu
ranije

478

phishing incidenata —
vodeća kategorija

To su samo prijavljeni i obrađeni incidenti — ne svi pokušaji i štete.

Izvor: CERT za 2025 godinu.

Zakon ne obuhvaća sve jednako, ali rizik obuhvaća sve

1

Izravni obveznici

Kategorizirani ključni i važni subjekti u propisanim sektorima.

2

Dobavljači obveznika

Sigurnosni zahtjevi dolaze kroz ugovore i lanac opskrbe.

3

Sve ostale tvrtke

Isti zastoј, prijevara, gubitak podataka i povjerenja kupaca.

Prvo pitanje nije: 'Kolika je kazna?' Prvo pitanje je: 'Koji je naš status i o kome naše poslovanje ovisi?'

18 minuta do pogrešne uplate

- **08:07** Stiže poruka: dobavljač je 'promijenio IBAN'.
- **08:19** Uplata je odobrena i poslana.
- **11:30** Pravi dobavljač pita zašto račun nije plaćen.

Tko je pogriješio?

Zaposlenik ili proces koji nije tražio provjeru?



Vanjski IT može održavati sustav. Ne može preuzeti odluke uprave.

Uprava mora **odobriti mjere**

Uprava mora **nadzirati provedbu**

Uprava mora **osigurati osposobljavanje**

24

sata

rano upozorenje

72

sata

početna
obavijest

30

dana

završno izvješće

Rokovi se odnose na značajne incidente kategoriziranih subjekata.

Uprava zadržava odgovornost; IT provodi mjere.

Backup postoji. Možemo li iz njega stvarno vratiti poslovanje?



Problem

Kopija je postojala, ali nisu bili poznati redoslijed povrata, stvarno trajanje i odgovorne osobe.

Kako smo pristupili

- odvojena sigurnosna kopija
- testni povrat podataka
- prioritet ključnih sustava
- kontaktni kanal izvan incidenta

Rezultat: poznat redoslijed i mjerljivo vrijeme oporavka.

Jedno zaraženo računalo ne smije zaustaviti pogon

Rizik

Uredska računala, strojevi i udaljeni pristup servisera bili su previše povezani.

Kako smo pristupili

- odvajanje uredske i proizvodne mreže
- vremenski ograničen pristup uz MFA
- evidencija udaljenih pristupa
- alternativni način rada

Rezultat: incident u uredu ne znači automatski prekid proizvodnje.



Radim normalno no drugi se žale



Problem

Tvrtka je „normalno i bez problema poslovala” no poslovni partneri su od njih primali fakture za neodrađene poslove.

Kako smo pristupili

- detaljna analiza i čišćenje cijelog sustava
- testni povrat podataka
- prioritet ključnih sustava
- uvedeni protokoli rada

Rezultat: poznati kada smo napadnuti i zaštititi sebe i druge

Poznati dobavljač

Rizik

Opuštenost prilikom rada s „poznatim” dobavljačem.

Kako smo pristupili

- zaposlenicima poslan lažni e-mail od poznatog dobavljača
- klikom na poveznicu dobili obavijest o napadu
- dobili objašnjenje kako su trebali i mogli prepoznati pokušaj prevare
- uvedeni protokoli rada

Rezultat: Educirani zaposlenici i uprava koji znaju kako prepoznati pokušaj prevare.



Napadač koristi AI. Obrana također mora.



AI napadaču

- uvjerljiviji personalizirani phishing
- sintetički glas i lažni identitet
- brže traženje ranjivosti

AI obrani

- otkriva neuobičajeno ponašanje
- povezuje i prioritizira upozorenja
- ubrzava analizu i odgovor stručnjaka

AI pojačava proces koji već imate — loš ili dobar.

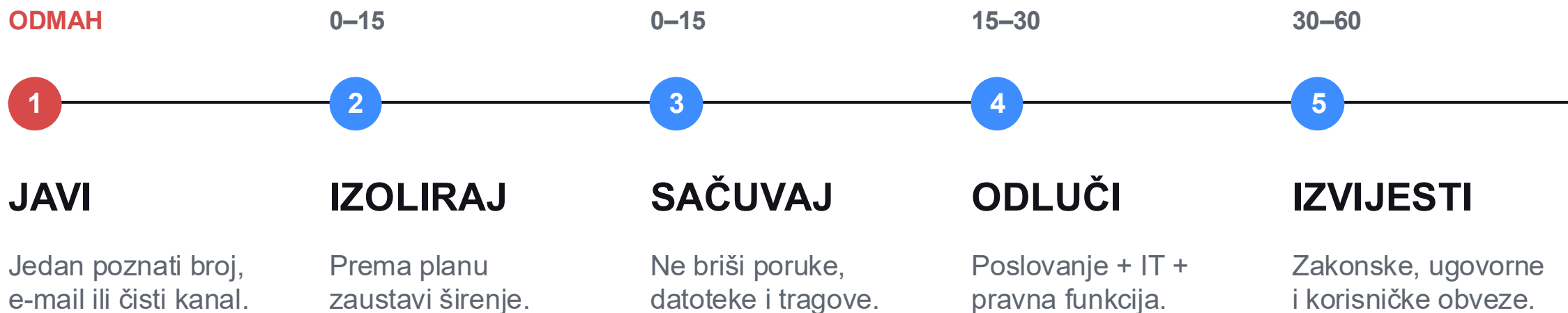
Najskuplja rečenica nije: ‘Kliknuo sam.’

Nego: ‘Nisam nikome rekao.’

Cilj edukacije nije savršenstvo.
Cilj je prijava u jednoj minuti.



Prvih 60 minuta mora biti uvježbano prije incidenta



Ako se tijekom incidenta prvi put raspravlja tko odlučuje i koga zovemo — već kasnimo.

Važan je dobro posložen proces



Jasne odgovornosti

brže odluke i brži odgovor na incident

Jedan izvor podataka

manje pogrešaka i jednostavnija kontrola

Standardno odobravanje

brža obrada i manji rizik prijevare

Automatiziran ulazak i izlazak

brže uključivanje ljudi i manje suvišnih prava

Manje rizika. Više učinka.

Postavite sebi ovih pet pitanja

- 1 Koja tri sustava moraju raditi da bismo mogli poslovati?

- 2 Koliko dugo možemo raditi bez njih?

- 3 Kada smo posljednji put stvarno vratili podatke iz kopije?

- 4 Kome zaposlenik javlja da je kliknuo na sumnjivu poveznicu?

- 5 Tko u prvih 60 minuta donosi poslovne odluke?

Sigurna tvrtka nije ona u kojoj nitko ne pogriješi — nego ona koja pogrešku brzo otkrije, prijavi i preživi.

CITUS-ov tim vam može pomoći

- 1 Početna procjena kibernetičke sigurnosti
- 2 Prioritetni akcijski plan
- 3 Tehničke i organizacijske mjere, uključujući AI obranu
- 4 Edukacija ljudi i uvježban protokol incidenta
- 5 **Manje zastoja. Manje rizika. Više produktivnosti.**



Javite nam se: citus@citus.hr • +385 1 3667 120 • [citus.hr](https://www.citus.hr)