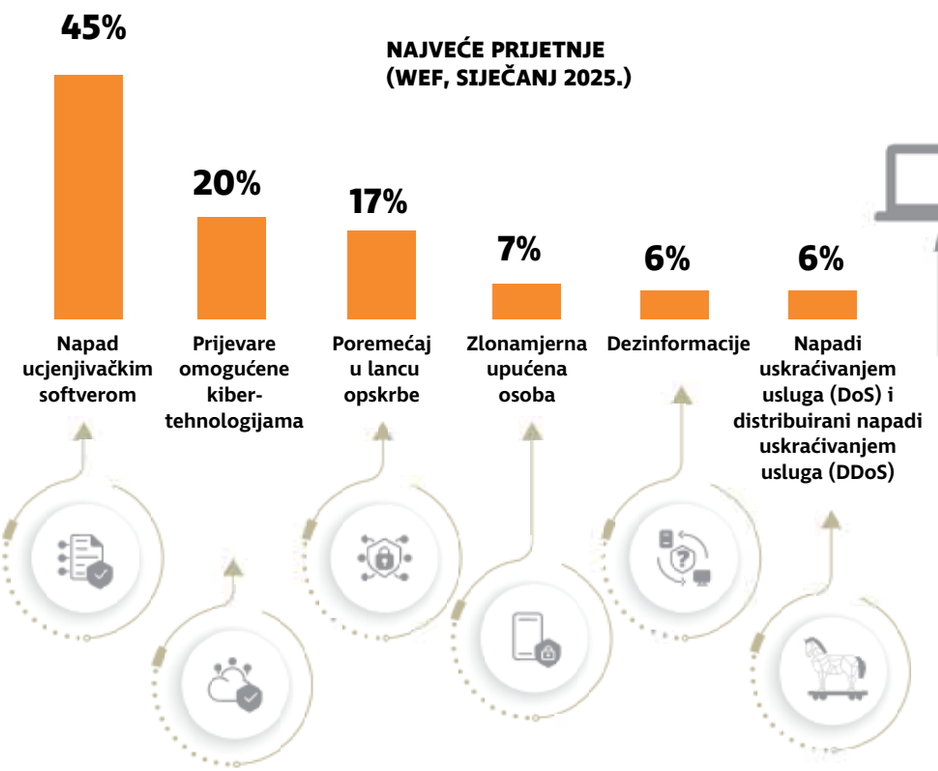

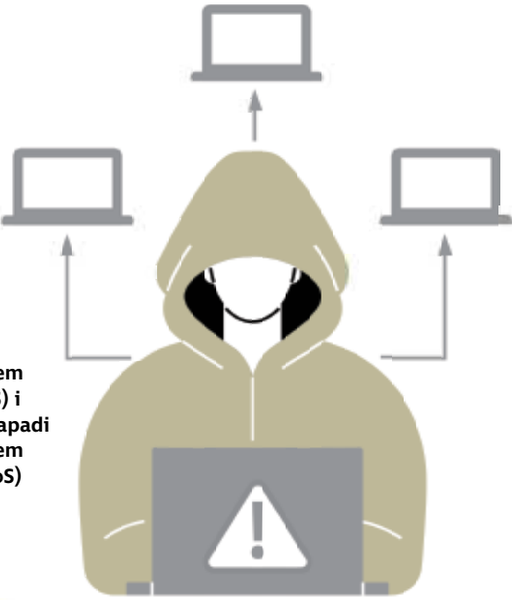

U vremenu povijesno gotovo nezabilježenih geopolitičkih promjena kojima svjedočimo, svi rizici ponovno se razmatraju. Kibernetički napadi postali su značajan segment općih poslovnih rizika. U vremenu modernih sukoba projiciranjem interesa zainteresiranih strana kibernetički napadi postaju posebno značajno područje jer nas mogu dovesti do gubitka poslovanja te financijskih i reputacijskih gubitaka. Razvoj novih tehnoloških sustava i napredne mogućnosti informatičkih tehnologija nude osim velikih prilika za napredak društva i alate kibernetičkim kriminalcima kakve do jučer nisu imali. Rađaju se nove mogućnosti prijevara, proboja sustava ili krađe podataka korištenjem novih metoda socijalnog inženjeringa za ulazak u vaše podatke. Novi alati umjetne inteligencije danas već proizvode zvučne, pa i videozapise kojima kopiraju identitete ključnih osoba pomoću kojih mogu uputiti nalog djelatnicima tvrtke da provedu neki poslovni zadatak, otkriju povjerljive podatke ili izvrše transakcije.

KAD SOFTVER POSTANE PRIJETNJA

U trenutku kada vaš posao počne ovisiti o IT rješenjima preuzimate i rizik da u softveru kao i opremi koju koristite već postoji opasna ranjivost, slabost koja nije poznata. Ako je otkriju istraživači kojima je to profesionalni izazov i prijave proizvođaču, često bivaju nagrađeni. Primjerice, u 2024. Google je isplatio ukupno 11,8 milijuna dolara za otkrivanje ranjivosti u svojim proizvodima. Iako je pad broja izvješća o ranjivostima zabilježen u razini od 8%, Google je objavio da je pritom otkriven za 2% veći broj kritičnih i visokorizičnih ranjivosti. Kao i ostali proizvođači softvera, Google će otkrivene ranjivosti, dakako, otkloniti u razumnom roku. No, što kada slabost otkriju kriminalci? Čuvat će to za sebe, pokušati pretvoriti slabost u nov način napada na vaš sustav, oteti podatke, zaključati ih i ucijeniti vas za visoku svotu! Takve slabosti, tzv. *zero-day vulnerabilities*, otkrivaju se svaki dan, pa je zato nužno pratiti objave i primjenjivati upute. No rizik i dalje ostaje i jedino što je preostalo jest prilagoditi se.

Kibernetička sigurnost ili digitalna otpornost, što je prioritet?

Ključna je priprema za incidente: prepoznati gdje se mogu dogoditi, kako će djelovati i što možete učiniti kako biste se brže i lakše oporavili i nastavili poslovati

UDAR NA CIJELU ORGANIZACIJU

Ključna je preporuka razvoj okvira za pripremu organizacije za incidente: prepoznati gdje se mogu dogoditi, kako će djelovati i što možete učiniti kako biste se brže i lakše oporavili i nastavili poslovati. Dobro i pouzdano uređen sustav rezervne pohrane podataka temelj je svakog plana oporavka, ali nije dovoljan. Incident zahvaća cijelu organizaciju te svi moraju biti svjesni što i kojim redoslijedom u takvoj situaciji trebaju činiti te kakvim se alatima i procesima služiti. Digitalna otpornost ne može se kupiti, ona se stječe sustavnim pripremama i učenjem cijele organizacije, dakako, na temeljima dobro uređenog IT sustava i stručnjaka koji upravljaju tehnologijama.
Za postizanje digitalne otpornosti potreban je kontinuiran rad, ulaganja i provjera rezultata na tom putu. Organizacije koje se preustroje i rade aktivno na postizanju digitalne otpornosti imaju znatno veće šanse opstati i preživjeti kibernetičke napade.