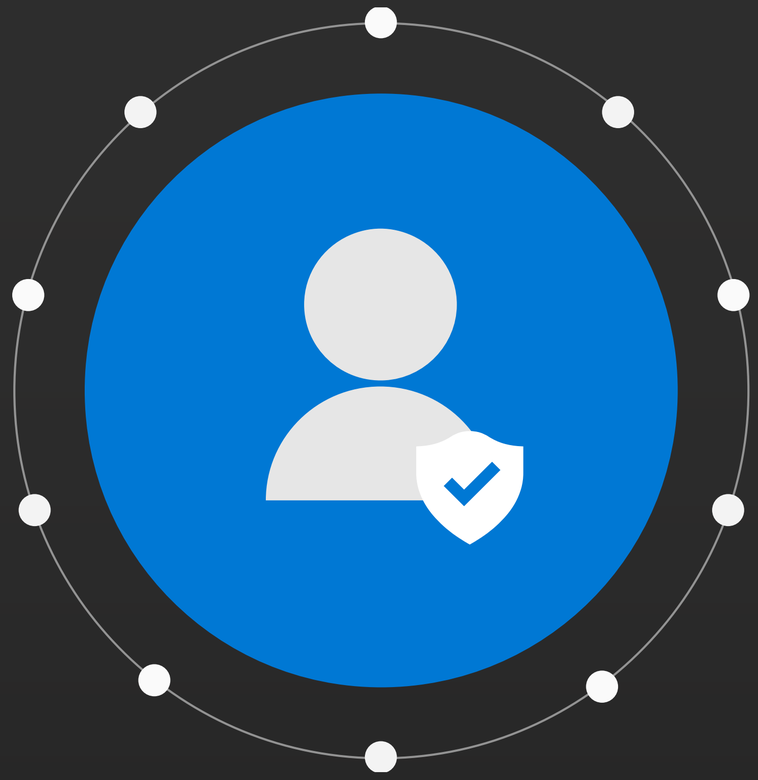
Microsoft 365

Deset saveta za omogućavanje bezbednosti modela nulte pouzdanosti



Deset saveta za omogućavanje bezbednosti modela nulte pouzdanosti

Bezbednosni modeli zasnovani na perimetru zastareli su usled rasprostranjenog usvajanja usluga u javnom oblaku i porasta mobilnosti radne snage. Aplikacije i podaci organizacije verovatno se nalaze i unutar tradicionalnog zaštitnog zida i izvan njega. Bezbednosni i IT timovi više ne mogu da pretpostavljaju da su korisnici i uređaji (lični i poslovni) na mreži bezbedniji od onih izvan nje. Kontrole perimetra tek donekle sprečavaju napadača da se kreće lateralno na mreži kad dobije početni pristup.

Neophodan je zaokret ka bezbednosti „bez granica“, obično poznatijoj kao nulta pouzdanost. U modelu nulte pouzdanosti svi korisnici i uređaji, bili oni na poslovnoj mreži ili van nje, smatraju se nepouzdanim. Pristup se dodeljuje na osnovu dinamičke procene rizika povezanog sa svakim zahtevom. Iste bezbednosne provere primenjuju se svakog puta na sve korisnike, uređaje, aplikacije i podatke.

Nulta pouzdanost hvata zamah

Postoji veliko interesovanje za model nulte pouzdanosti. Nova anketa organizacije IDG pokazuje da je 21% organizacija već usvojilo model nulte pouzdanosti, dok 63% planira to da uradi u toku narednih 12 meseci[1]. U zasebnoj anketi „Bezbednosni prioriteti“ organizacije IDG 2018. godine, 35% organizacija navelo je da planira da poveća ulaganje u model nulte pouzdanosti ili da za nju uvede novu kategoriju troškova. Drugih 30% vidi nultu pouzdanost kao potencijalnu novu oblast za ulaganja[2].

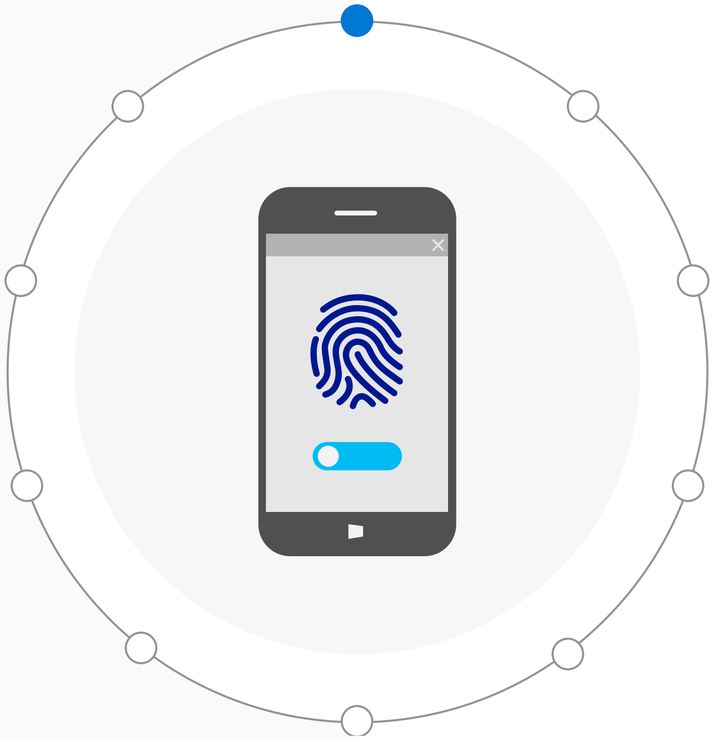
Iako nulta pouzdanost uzima zalet, to nije novi pristup. Bezbednosni konzorcijum pod imenom Jericho Forum osnovan je 2004. kako bi promovisao ideju „deperimetrizacije“ tj. usredsređivanja na pronalaženje načina za zaštitu podataka na novim platformama[3]. Analitičko preduzeće Forrester skovalo je termin „Nulta pouzdanost“ 2010[4].

Interesovanje za nultu pouzdanost nedavno je poraslo, pogotovo među organizacijama koje traže način za sprečavanje napadača da se kreću lateralno na mreži.

Dostizanje modela nulte pouzdanosti može da iziskuje godine truda i saradnju širom celog preduzeća. Ako ste posvećeni primeni modela nulte pouzdanosti odnosno čak i ako ga samo razmatrate, evo 10 saveta koji bar malo pojednostavljuju taj proces.

1. savet

Ponovno usklađivanje na osnovu identiteta



Najbolja polazna tačka za nultu pouzdanost jeste identitet.

Korisnici mogu da imaju više uređaja i da pristupaju resursima preduzeća sa raznih mreža i pomoću različitih aplikacija.

1. savet

Ponovno usklađivanje na osnovu identiteta

Najbolja polazna tačka za nultu pouzdanost jeste identitet.

Korisnici mogu da imaju više uređaja i da pristupaju resursima preduzeća sa raznih mreža i pomoću različitih aplikacija. Pristup skoro svim tim resursima zahteva potvrdu identiteta, što identitet čini osnovnim zajedničkim elementom svih zahteva za pristup, bez obzira na to da li potiču sa ličnog uređaja na javnoj Wi-Fi mreži ili sa poslovnog uređaja unutar mrežnog perimetra. Kad koriste identitet kao nivo kontrole, preduzeća mogu da tretiraju svaki zahtev za pristup kao nepouzdan dok se potpuno ne ispitaju korisnik, uređaj i ostali faktori.

Mnoge organizacije se usredsređuju na mikrosegmentaciju kao pristup omogućavanju nulte pouzdanosti, ali taj pristup ima znatna ograničenja.

Mikrosegmentacija može da bude korisna za smanjenje površine napada i za zaustavljanje daljeg bezbednosnog proboja unutar zastarelih lokalnih okruženja aplikacija.

Ali taj pristup je manje efikasan u okruženjima u oblaku, gde IT sektor često nije vlasnik mreža između poslovnih resursa i ne upravlja njima.

Nulta pouzdanost predstavlja kulturološki prelazak sa kontrola zasnovanih na mreži na smernice i procese zasnovane na identitetu. Timovi u specijalizovanim silosima treba da se usaglase sa zaštitom zasnovanom na identitetu kako bi postavili temelje za model nulte pouzdanosti. „Postavljanje temelja za identitet predstavlja najbolju polaznu tačku“, kaže Mark Simos, glavni arhitekta grupe za rešenja za kibernetičku bezbednost korporacije Microsoft. „To vam pruža dobar mrežni prolaz za pristup između resursa i potencijalnih pretnji po njih.“

2. savet

Primena kontrola uslovnog pristupa

Hakeri redovno ugrožavaju akreditive za identitet i koriste ih za pristup sistemima i lateralno kretanje na mreži.

Stoga se o pouzdanosti ne može zaključivati samo na osnovu toga da li se određeni korisnik ili uređaj nalaze unutar ili izvan poslovne mreže.

2. savet

Primena kontrola uslovnog pristupa

Hakeri redovno ugrožavaju akreditive za identitet i koriste ih za pristup sistemima i lateralno kretanje na mreži.

Stoga se o pouzdanosti ne može zaključivati samo na osnovu toga da li se određeni korisnik ili uređaj nalaze unutar ili izvan poslovne mreže.

Umesto toga, **usvojite takav način razmišljanja da uvek „pretpostavljate da je to bezbednosni proboj“ i ne verujte nijednom zahtevu dok se potpuno ne ispita.** Za model nulte pouzdanosti, odluke prilikom kontrole pristupa treba da budu dinamične i da se uslovno dodeljuju na osnovu procene i kontekstualnog shvatanja rizika povezanog sa svakim zahtevom za resursima u više dimenzija.

Takav stav prema uslovnom pristupu razmatra identitet korisnika, prava pristupa, ispravnost uređaja, aplikaciju i bezbednost mreže, kao i osetljivost podataka kojima se pristupa.

Zatim se koristi mašina za nametanje vođena skupom preciznih smernica kako bi se odlučilo da li da se dozvoli, ograniči ili blokira pristup traženom resursu. Mreža nulte pouzdanosti sa odgovarajućim smernicama za uslovni pristup za korisnike i uređaje može da spreči hakere da koriste ukradene akreditive za lateralno kretanje na mreži.

3. savet

Ojačavanje akreditiva

Slabe lozinke narušavaju bezbednost sistema identiteta i olakšavaju hakerima da ugroze mrežu, na primer preko napada putem rasejavanja lozinke ili pretrpavanja akreditivima.

3. savet

Ojačavanje akreditiva

Slabe lozinke narušavaju bezbednost sistema identiteta i olakšavaju hakerima da ugroze mrežu, na primer preko napada putem rasejavanja lozinke ili pretrpavanja akreditivima.

Ako višestruku potvrdu identiteta uvrstite u ograničenja uslovnog pristupa, možete da poboljšate verifikaciju korisnika i ograničite mogućnost hakera da zloupotrebe ukradene akreditive.

To pruža dodatni sloj provere valjanosti korisnika, posebno za pružanje pristupa aplikacijama i podacima od presudne važnosti.

4. savet

Plan strategije dvojnog perimetra

Kako biste sprečili zastoje u poslovanju i ponovno uvođenje starih rizika, zadržite postojeće zaštite zasnovane na mreži kad u okruženje dodate nove kontrole zasnovane na identitetu.

4. savet

Plan strategije dvojnog perimetra

Kako biste sprečili zastoje u poslovanju i ponovno uvođenje starih rizika, zadržite postojeće zaštite zasnovane na mreži kad u okruženje dodate nove kontrole zasnovane na identitetu.

„U kontekstu nulte pouzdanosti zaista morate da počnete da gledate na aplikacije kao na one u oblaku ili one koje su zastarele“, kaže Simos. Aplikacije koje su izvorno u oblaku podržavaju kontrole zasnovane na identitetu i omogućavaju relativno lako postavljanje slojevitih pravila uslovnog pristupa.

Druga kategorija se sastoji od aplikacija koje su dizajnirane da budu iza zaštitnih zidova mreže u zastarelim okruženjima.

Te aplikacije zahtevaju modernizaciju kako bi podržavale uslovni pristup zasnovan na identitetu. Jedna opcija da to uradite u odgovarajućoj razmeri jeste da omogućite pristup preko bezbednog mrežnog prolaza za potvrdu identiteta ili proxy servera aplikacija, što omogućava i da uklonite VPN mreže (čime smanjujete rizik).

5. savet

Integracija obaveštavanja i analitike ponašanja

Podrška za kontrolu pristupa zasnovanu na identitetu u aplikacijama u oblaku nije jedini razlog da ubrzate migraciju u oblak.

Oblak generiše i obogaćeniju telemetriju kako bi omogućio bolje odluke prilikom kontrole pristupa. Na primer, takva telemetrija može da proširi kontrole uslovnog pristupa tako što će olakšati otkrivanje nestandardnog ponašanja korisnika ili entiteta radi otkrivanja pretnji.

5. savet

Integracija obaveštavanja i analitike ponašanja

Podrška za kontrolu pristupa zasnovanu na identitetu u aplikacijama u oblaku nije jedini razlog da ubrzate migraciju u oblak.

Oblak generiše i obogaćeniju telemetriju kako bi omogućio bolje odluke prilikom kontrole pristupa. Na primer, takva telemetrija može da proširi kontrole uslovnog pristupa tako što će olakšati otkrivanje nestandardnog ponašanja korisnika ili entiteta radi otkrivanja pretnji.

Mogućnost donošenja dobrih odluka prilikom kontrole pristupa zavisi od kvaliteta, kvantiteta i raznolikosti signala koji se integrišu u takvim odlukama.

Na primer, integrisanje izvora obaveštavanja o pretnjama, kao što su IP adrese za robote ili malver, prisiljava protivnike da neprestano nabavljaju nove resurse. Integrisanje dodatnih detalja o prijavljivanju (vreme, lokacija itd.) i proveravanje da li se oni podudaraju sa uobičajenom rutinom korisnika otežava napadačima da je oponašaju i smanjuje neugodnost za korisnike.

6. savet

Smanjenje površine napada

Da biste poboljšali bezbednost infrastrukture identiteta, važno je da smanjite površinu napada. (To je, naravno, dobra bezbednosna praksa i uopšte.)

Na primer, primena upravljanja privilegovanim identitetima smanjuje verovatnoću da će se ugroženi nalog koristiti u ulozi administratora ili drugoj privilegovanoj ulozi.

6. savet

Smanjenje površine napada

Da biste poboljšali bezbednost infrastrukture identiteta, važno je da smanjite površinu napada. (To je, naravno, dobra bezbednosna praksa i uopšte.)

Na primer, primena upravljanja privilegovanim identitetima smanjuje verovatnoću da će se ugroženi nalog koristiti u ulozi administratora ili drugoj privilegovanoj ulozi.

Dobra ideja je i da blokirate aplikacije koje koriste zastarele protokole za potvrdu identiteta.

To je od presudne važnosti jer ti protokoli ne podržavaju uslovni pristup niti višestruku potvrdu identiteta, što napadačima omogućava da ih zaobiđu.

Pored toga, ograničite ulazne tačke pristupa za potvrdu identiteta da biste kontrolisali način na koji korisnici pristupaju aplikacijama i resursima. To doprinosi i smanjenju uticaja koji imaju ugroženi akreditivi.

7. savet

Povećavanje svesti o bezbednosti

Infrastruktura identiteta i krajnje tačke može da generiše mnoštvo događaja vezanih za bezbednost i bezbednosna upozorenja.

Koristite sistem upravljanja bezbednosnim informacijama i događajima (SIEM) da biste prikupljali podatke i utvrđivali im korelaciju radi lakšeg otkrivanja sumnjivih aktivnosti i obrazaca koji ukazuju na potencijalne upade na mrežu i događaje kao što su iscureli akreditivi, loše IP adrese i pristup putem zaraženih uređaja**.**

7. savet

Povećavanje svesti o bezbednosti

Infrastruktura identiteta i krajnje tačke može da generiše mnoštvo događaja vezanih za bezbednost i bezbednosna upozorenja.

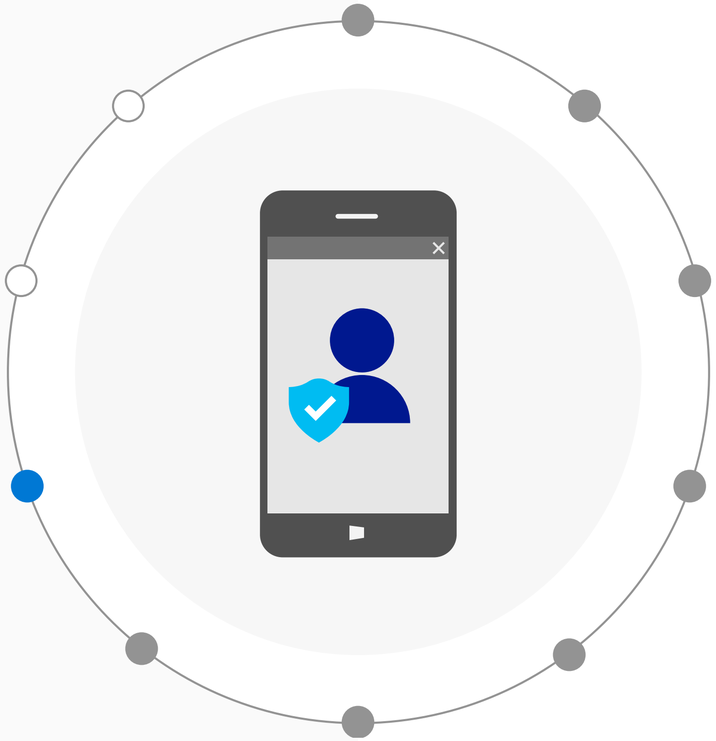
Koristite sistem upravljanja bezbednosnim informacijama i događajima (SIEM) da biste prikupljali podatke i utvrđivali im korelaciju radi lakšeg otkrivanja sumnjivih aktivnosti i obrazaca koji ukazuju na potencijalne upade na mrežu i događaje kao što su iscureli akreditivi, loše IP adrese i pristup putem zaraženih uređaja**.**

Sistem SIEM može da se koristi za nadgledanje aktivnosti korisnika i usaglašenosti dokumenata sa zakonskim zahtevima i kao pomoć prilikom forenzičke analize.

On može i da poboljša nadgledanje pristupa sa najmanje privilegija i obezbedi da korisnici imaju pristup samo resursima koji su im zaista neophodni.

8. savet

Omogućavanje samopomoći za krajnje korisnike



Korisnicima će verovatno mnogo više odgovarati nulta pouzdanost nego mnoge druge bezbednosne inicijative.

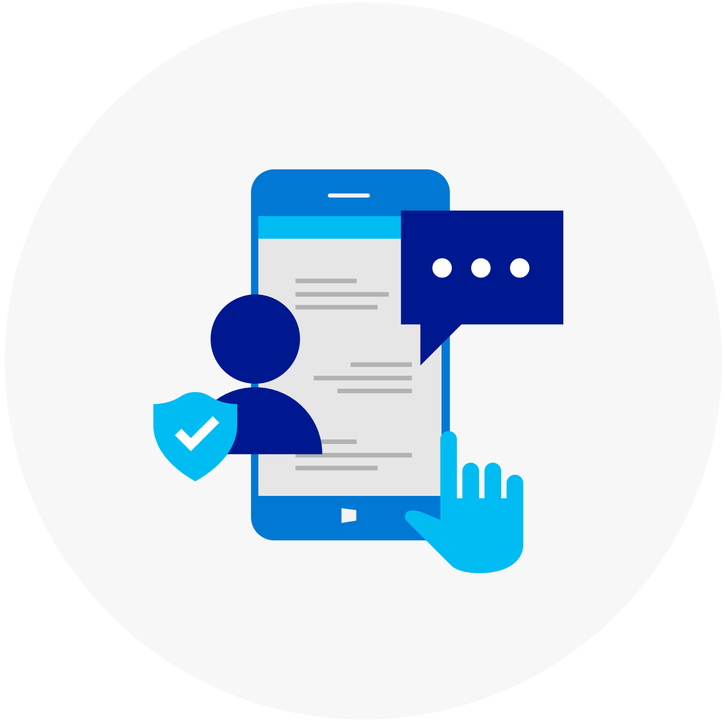
To je zbog toga što su već upoznati sa pristupom zasnovanim na identitetu na ličnim uređajima i u ličnim aplikacijama i žele isti utisak pri radu na poslu. Nulta pouzdanost bezbednosnim organizacijama omogućava da zaštite (i usvoje) moderne scenarije produktivnosti kao što su mobilni uređaji, BYOD i SaaS aplikacije, pri čemu su korisnici zadovoljni bez ugrožavanja bezbednosti.

8. savet

Omogućavanje samopomoći za krajnje korisnike

Korisnicima će verovatno mnogo više odgovarati nulta pouzdanost nego mnoge druge bezbednosne inicijative.

To je zbog toga što su već upoznati sa pristupom zasnovanim na identitetu na ličnim uređajima i u ličnim aplikacijama i žele isti utisak pri radu na poslu. Nulta pouzdanost bezbednosnim organizacijama omogućava da zaštite (i usvoje) moderne scenarije produktivnosti kao što su mobilni uređaji, BYOD i SaaS aplikacije, pri čemu su korisnici zadovoljni bez ugrožavanja bezbednosti.



IT timovi mogu da smanje zastoje podsticanjem korisnika da obavljaju određene zadatke vezane za bezbednost, kao što je samouslužno vraćanje lozinke.

Ako korisnicima omogućite da vraćaju ili otključavaju lozinke naloga bez pomoći administratora – uz nadgledanje toga da li ima zloupotrebe – obezbeđujete odgovarajuću ravnotežu između bezbednosti i produktivnosti.

Slično tome, primena samouslužnog upravljanja grupom vlasnicima omogućava da prave grupe i upravljaju njima bez potrebe da to obavlja administrator.

9. savet

Bez prevelikih obećanja

Nulta pouzdanost nije jedna „revolucionarna“ inicijativa kao što je to primena višestruke potvrde identiteta.

U pitanju je dugoročna završna faza sa novom generacijom bezbednosnih kontrola napravljenih potpuno drugačije od tradicionalnih modela pristupa zasnovanih na mreži.

9. savet

Bez prevelikih obećanja

Nulta pouzdanost nije jedna „revolucionarna“ inicijativa kao što je to primena višestruke potvrde identiteta.

U pitanju je dugoročna završna faza sa novom generacijom bezbednosnih kontrola napravljenih potpuno drugačije od tradicionalnih modela pristupa zasnovanih na mreži.

Ostvarivanje vizije putem neprekidnog niza manjih projekata iziskuje vreme.

Važno je da usput na odgovarajući način postavljate očekivanja i upravljate njima. Zadobijte podršku najvažnijih zainteresovanih strana i pripremite plan za efikasno komuniciranje s njima tokom životnog ciklusa projekta. Pripremite se da preduzmete korake kako biste prevazišli kulturološki otpor i druge izazove koje postavljaju grupe koje su već dugo navikle da rade na veoma drugačiji način.

10. savet

Pokazivanje vrednosti s vremenom

Jedan od najefikasnijih načina za dobijanje dugoročne podrške za inicijativu nulte pouzdanosti jeste da pokažete porast vrednosti od svake investicije.

Više od polovine ispitanika (51%) u anketi organizacije IDG o bezbednosti reklo je da bi model pristupa nulte pouzdanosti doprineo poboljšanju mogućnosti da zaštite podatke klijenta, a 46% reklo je da bi on omogućio vrhunski i bezbedniji utisak krajnjeg korisnika pri radu.

10. savet

Pokazivanje vrednosti s vremenom

Jedan od najefikasnijih načina za dobijanje dugoročne podrške za inicijativu nulte pouzdanosti jeste da pokažete porast vrednosti od svake investicije.

Više od polovine ispitanika (51%) u anketi organizacije IDG o bezbednosti reklo je da bi model pristupa nulte pouzdanosti doprineo poboljšanju mogućnosti da zaštite podatke klijenta, a 46% reklo je da bi on omogućio vrhunski i bezbedniji utisak krajnjeg korisnika pri radu.

Mogućnost donošenja dobrih odluka prilikom kontrole pristupa zavisi od kvaliteta, kvantiteta i raznolikosti signala koji se integrišu u takvim odlukama.

Na primer, integrisanje izvora obaveštavanja o pretnjama, kao što su IP adrese za robote ili malver, prisiljava protivnike da neprestano nabavljaju nove resurse. Integrisanje dodatnih detalja o prijavljivanju (vreme, lokacija itd.) i proveravanje da li se oni podudaraju sa uobičajenom rutinom korisnika otežava napadačima da je oponašaju i smanjuje neugodnost za korisnike.

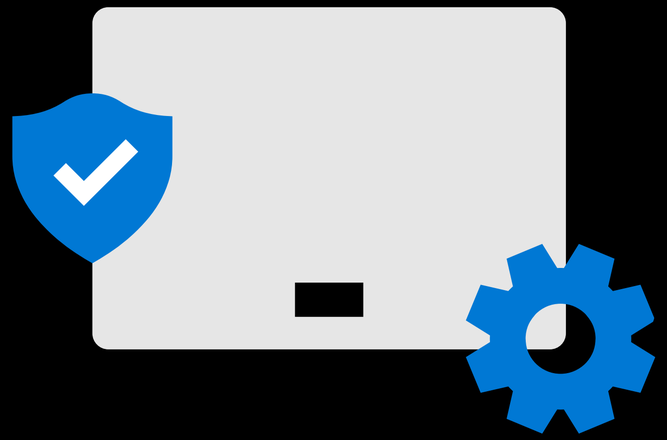
Microsoft 365

Model budućnosti

Nije moguće predvideti koje nove zloupotrebe mogu da iskrsnu u svako doba ili način na koji se može dobiti pristup vašem okruženju. Zbog toga što nikada ne možete pretpostavljati da su korisnik odnosno uređaj, aplikacija ili mreža koje koristi potpuno zaštićeni, jedini razuman pristup bezbednosti jeste da ne verujete ničemu, već da sve verifikujete.

Model nulte pouzdanosti nije lako dostići, ali on je osnovni element svakog dugoročnog cilja modernizacije velikih digitalnih preduzeća.

Saznajte više o tome kako da spremno dočekate izazove u vezi sa kibernetičkom bezbednošću:



Posetite seriju CISO Spotlight

[1] Istraživačka anketa organizacije IDG, maj 2019.
[2] Istraživanje organizacije IDG o bezbednosnim prioritetima, 2018, https://www.idg.com/tools-for-marketers/2018-security-priorities-study/
[3] Wikipedia, https://en.wikipedia.org/wiki/Jericho_Forum
[4] CSO, jul 2018, https://www.csoonline.com/article/3287057/what-it-takes-to-build-a-zero-trust-network.html