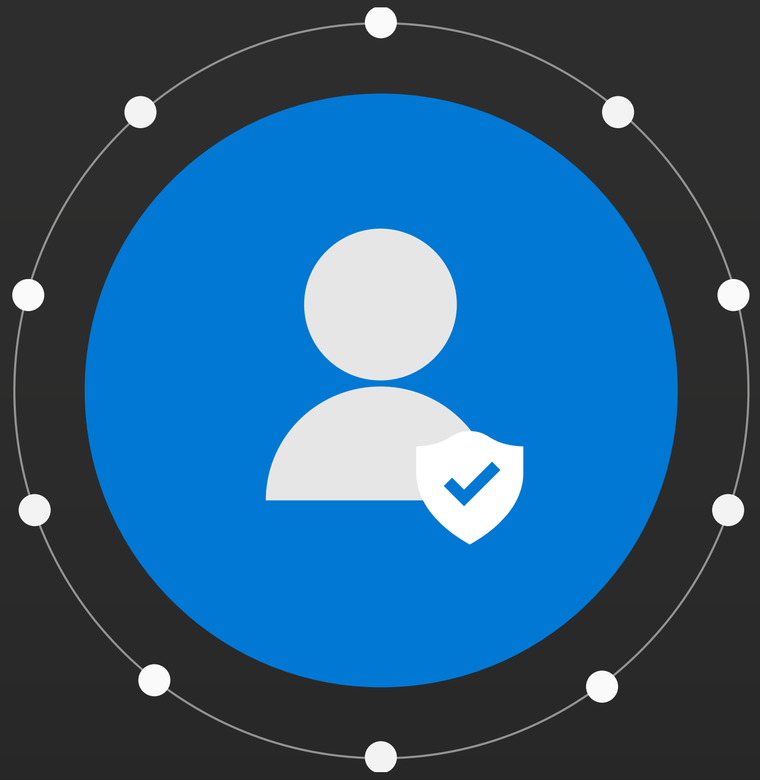
Microsoft 365

10 sfaturi pentru activarea securității Zero Trust



10 sfaturi pentru activarea securității Zero Trust

Adoptarea pe scară largă a serviciilor cloud publice și dezvoltarea forței de muncă mobile au făcut ca modelele de securitate bazate pe perimetru să fie depășite. Aplicațiile și datele unei organizații vor exista probabil atât în interiorul firewallului tradițional, cât și în afara acestuia. Echipele de securitate și IT nu mai pot presupune că utilizatorii și dispozitivele lor (atât personale, cât și de corporație) din rețea sunt mai sigure decât cele din afară. Controalele de perimetru fac puțin pentru a împiedica un atacator să se deplaseze prin rețea după ce obține acces inițial la aceasta.

Este necesar un pivot la securitate „nelimitată", cunoscut mai frecvent sub numele de Zero Trust. În cadrul unui model Zero Trust, toți utilizatorii și toate dispozitivele, atât din interiorul, cât și din afara rețelei de corporație, nu sunt considerați de încredere. Accesul se acordă doar pe baza unei evaluări dinamice a riscului asociat cu fiecare solicitare. Aceleași verificări de securitate se aplică tuturor utilizatorilor, dispozitivelor, aplicațiilor și datelor de fiecare dată.

Zero Trust câștigă teren

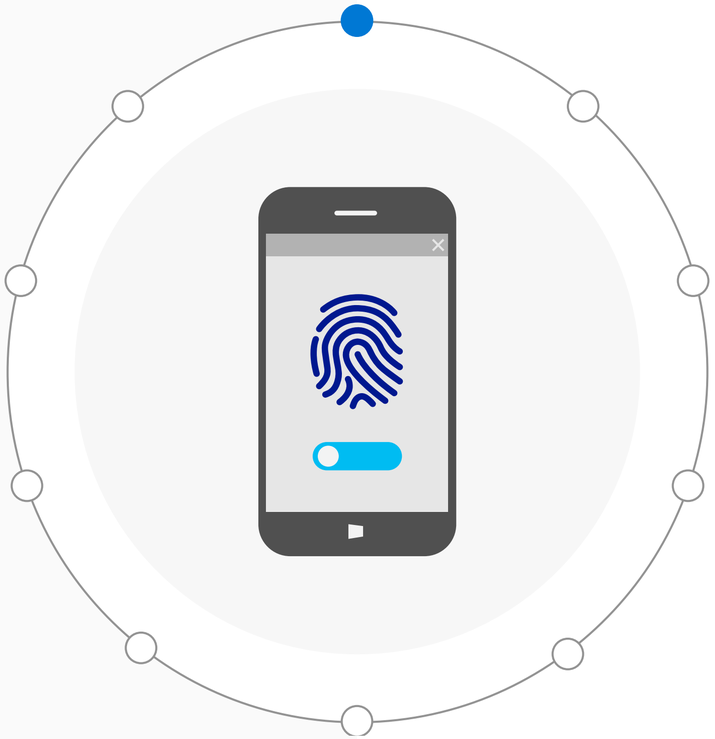
Interesul pentru Zero Trust este puternic. Conform unei noi anchete IDG, 21% dintre organizații au adoptat deja un model Zero Trust, iar 63% au planificat să facă acest lucru în următoarele 12 luni [1]. Într-o anchetă separată, Priorități de securitate 2018, de la IDG, 35% din organizații au declarat că intenționează să aloce sume mai mari pentru Zero Trust sau să creeze o categorie de cheltuieli pentru acesta. Alte 30% au considerat Zero Trust drept o nouă zonă de investiții potențială[2].

Deși Zero Trust capătă amploare, abordarea nu este nouă. În 2004 s-a format Jericho Forum, un consorțiu de securitate, cu scopul de a promova ideea de „deperimetrizare", care se concentrează asupra găsirii de soluții pentru a proteja datele de pe platforme noi[3]. Firma de analiști Forrester a inventat termenul „Zero Trust" în 2010[4]. Interesul pentru Zero Trust a crescut recent, mai ales în rândul organizațiilor care caută o modalitate de a-i împiedica pe atacatori să se miște lateral în rețea.

Trecerea la un model Zero Trust poate însemna eforturi depuse ani la rând și necesită colaborare la nivelul întreprinderii. Dacă v-ați hotărât să implementați un model Zero Trust sau dacă deocamdată doar vă gândiți la aceasta, iată 10 sfaturi pentru a vă înlesni această călătorie.

Sfat 01

Realinierea în jurul identității



Identitatea este cel mai bun punct de plecare pentru Zero Trust.

Utilizatorii pot să aibă mai multe dispozitive și să acceseze resurse de întreprindere dintr-o varietate de rețele și aplicații.

Sfat 01

Realinierea în jurul identității

Identitatea este cel mai bun punct de plecare pentru Zero Trust.

Utilizatorii pot să aibă mai multe dispozitive și să acceseze resurse de întreprindere dintr-o varietate de rețele și aplicații. Aproape toate aceste resurse necesită autentificare, făcând identitatea un numitor comun în toate solicitările de acces, fie de pe un dispozitiv personal de pe o rețea Wi-Fi publică, fie de pe un dispozitiv de corporație din perimetrul rețelei. Utilizarea identității ca nivel de control le permite companiilor să trateze fiecare solicitare de acces ca nefiind de încredere până când utilizatorul, dispozitivul și ceilalți factori sunt complet examinați.

Multe organizații se concentrează pe microsegmentare ca pe o abordare a activității Zero Trust, dar această abordare are limitări semnificative.



Microsegmentarea poate fi utilă la reducerea suprafețelor de atac și pentru izolarea brеșei în mediile de aplicație moștenite la nivel local.

Totuși, această abordare nu este atât de eficientă în mediile cloud în care rețelele dintre activele de întreprindere adesea nu sunt deținute sau gestionate de IT.

Zero Trust reprezintă o trecere culturală de la controalele bazate pe rețea la politicile și procesele bazate pe identitate. Echipele din structurile specializate trebuie să se alinieze în jurul protecției bazate pe identitate pentru a pune bazele unui model Zero Trust. „Construirea bazei pentru identitate este cel mai bun punct de plecare”, afirmă Mark Simos, arhitect coordonator în cadrul Grupului de soluții de securitate cibernetică Microsoft. „Acesta vă oferă un gateway de acces corespunzător între active și potențialele amenințări la adresa acestora.”

Sfat 02

Punerea în aplicare a controalelor de acces condiționat



Hackerii compromit, de obicei, acreditările de identitate și le utilizează pentru a accesa sistemele și pentru a se deplasa lateral în rețea.

Prin urmare, încrederea nu poate fi dedusă doar din faptul că un anumit utilizator sau dispozitiv al său se află în interiorul sau în afara rețelei de corporație.

Sfat 02

Punerea în aplicare a controalelor de acces condiționat

Hackerii compromit, de obicei, acreditările de identitate și le utilizează pentru a accesa sistemele și pentru a se deplasa lateral în rețea.

Prin urmare, încrederea nu poate fi dedusă doar din faptul că un anumit utilizator sau dispozitiv al său se află în interiorul sau în afara rețelei de corporație.

În schimb, **adoptați mentalitatea „presupunem o breșă” și nu aveți încredere în nicio solicitare până când nu este complet examinată.** Pentru Zero Trust, deciziile de control al accesului ar trebui să fie dinamice și acordate în funcție de evaluarea și înțelegerea contextuală a riscului asociat cu fiecare solicitare de resurse pe mai multe dimensiuni.



Această abordare a accesului condiționat analizează identitatea utilizatorului și drepturile de acces, starea dispozitivelor, siguranța aplicațiilor și a rețelei, precum și gradul de confidențialitate al datelor accesate.

Un motor de impunere, ghidat de un set de politici granulare, este apoi utilizat pentru a decide dacă să permită, să restricționeze sau să blocheze accesul la resursa solicitată. O rețea Zero Trust cu politicile corecte de acces condiționat pentru utilizatori și dispozitive poate împiedica hackerii să utilizeze acreditările furate pentru a se deplasa lateral în rețea.

Sfat 03

Consolidați-vă acreditările



Parolele slabe subminează securitatea sistemului de identitate și le permit hackerilor să vă compromită ușor rețeaua, de exemplu, prin atacuri de tip spray asupra parolelor sau de tip „credential-stuffing”.

Sfat 03

Consolidați-vă acreditările

Parolele slabe subminează securitatea sistemului de identitate și le permit hackerilor să vă compromită ușor rețeaua, de exemplu, prin atacuri de tip spray asupra parolelor sau de tip „credential-stuffing”.



Introducerea autentificării multi-factor ca parte a restricțiilor de acces condiționat poate favoriza o mai bună verificare a utilizatorului și poate limita capacitatea hackerilor de a utiliza în mod abuziv acreditări furate.

Acesta asigură un nivel suplimentar de validare a utilizatorului, mai ales pentru acordarea accesului la aplicații și date critice.

Sfat 04

Planificați o strategie cu perimetru dublu



Pentru a preveni perturbarea afacerii și reintroducerea unor riscuri vechi, mențineți protecțiile bazate pe rețea adăugând în același timp noi controale pe baza identității la mediul dvs.

Sfat 04

Planificați o strategie cu perimetru dublu

Pentru a preveni perturbarea afacerii și reintroducerea unor riscuri vechi, mențineți protecțiile bazate pe rețea adăugând în același timp noi controale pe baza identității la mediul dvs.

„Într-un context Zero Trust, trebuie efectiv să începeți să priviți aplicațiile dvs. ca fiind cloud sau moștenite”, spune Simos. Aplicațiile native în cloud acceptă controale pe baza identității și permit ca regulile de acces condiționat să fie stratificate relativ ușor.



Cealaltă categorie cuprinde aplicații care au fost proiectate să stea în spatele firewallurilor de rețea în mediile moștenite.

Aceste aplicații necesită modernizare pentru a susține accesul condiționat pe baza identității. O opțiune pentru a face acest lucru la scară este să activați accesul printr-un gateway de autentificare sau proxy pentru aplicații securizat, ceea ce vă poate permite, de asemenea, să eliminați VPN-urile (ceea ce vă poate reduce riscul).

Sfat 05

Integrați analize de investigare și de comportament



Suportul pentru controlul accesului pe baza identității în aplicațiile cloud nu este singurul motiv pentru a accelera migrarea în cloud.

Mediul cloud generează, de asemenea, o telemetrie mai bogată pentru a permite luarea unor decizii mai bune privind controlul accesului. De exemplu, o astfel de telemetrie poate spori controalele de acces condiționat făcând mai ușor de dedus un comportament anormal al utilizatorului sau entității pentru a identifica amenințările.

Sfat 05

Integrați analize de investigare și de comportament

Suportul pentru controlul accesului pe baza identității în aplicațiile cloud nu este singurul motiv pentru a accelera migrarea în cloud.

Mediul cloud generează, de asemenea, o telemetrie mai bogată pentru a permite luarea unor decizii mai bune privind controlul accesului. De exemplu, o astfel de telemetrie poate spori controalele de acces condiționat făcând mai ușor de dedus un comportament anormal al utilizatorului sau entității pentru a identifica amenințările.



Capacitatea dvs. de a lua decizii bune privind controlul accesului depinde de calitatea, cantitatea și diversitatea semnalelor pe care le integrați în acele decizii.

De exemplu, integrarea unor surse de investigare a amenințărilor, cum ar fi adrese IP pentru programe bot sau malware, va forța adversarii să obțină în permanență resurse noi. Integrarea mai multor detalii despre conectare (oră, locație etc.) urmărind apoi dacă aceasta corespunde cu rutina normală a utilizatorului va fi mai greu de imitat pentru atacatori, reducând în același timp neplăcerile utilizatorului.

Sfat 06

Reduceți suprafața de atac



Pentru a consolida securitatea infrastructurii aferente identității, este important să reduceți suprafața de atac. (Desigur, aceasta este o bună practică de securitate în general.)

De exemplu, implementarea Privileged Identity Management va reduce probabilitatea de utilizare a unui cont compromis într-un rol de administrator sau într-un alt rol privilegiat.

Sfat 06

Reduceți suprafața de atac

Pentru a consolida securitatea infrastructurii aferente identității, este important să reduceți suprafața de atac. (Desigur, aceasta este o bună practică de securitate în general.)

De exemplu, implementarea Privileged Identity Management va reduce probabilitatea de utilizare a unui cont compromis într-un rol de administrator sau într-un alt rol privilegiat.



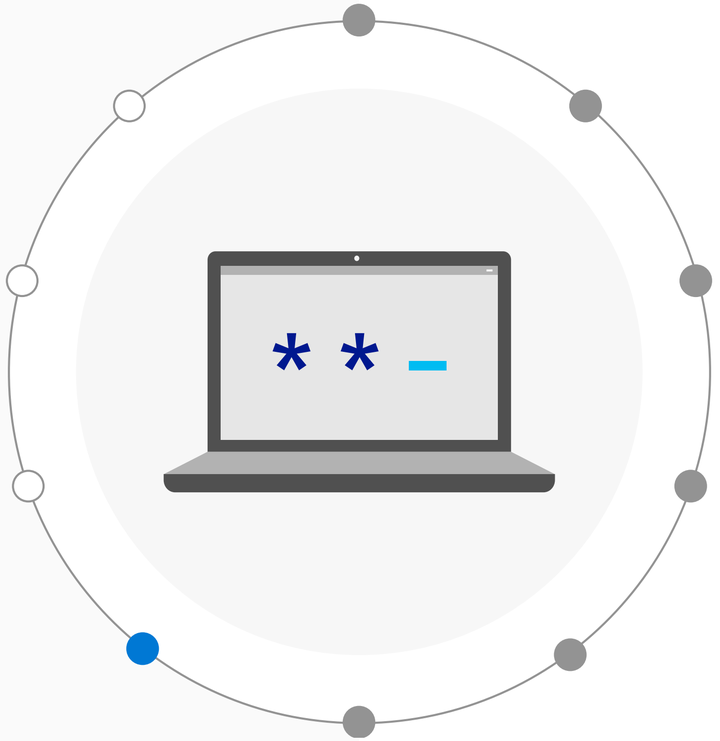
E o idee bună, de asemenea, să blocați aplicațiile utilizând protocoale de autentificare moștenite.

Acest lucru este esențial, deoarece aceste protocoale nu acceptă accesul condiționat sau autentificarea multi-factor, care permit atacatorilor să le ocolească.

În plus, limitați punctele de intrare de acces de autentificare pentru a controla modul în care utilizatorii accesează aplicațiile și resursele. Acest lucru vă va ajuta să reduceți și impactul acreditărilor compromise.

Sfat 07

Măriți nivelul de conștientizare privind securitatea



Infrastructura identității și a punctului final poate genera un volum mare de evenimente și avertizări de securitate.

Utilizați un sistem Managementul evenimentelor și informațiilor de securitate (SIEM) pentru a agrega și a corela datele astfel încât să detectați mai bine activități și modele suspecte care indică posibile intruziuni în rețea și evenimente, cum ar fi acreditări divulgate, adrese IP eronate și accesul de pe dispozitive infectate.

Sfat 07

Măriți nivelul de conștientizare privind securitatea

Infrastructura identității și a punctului final poate genera un volum mare de evenimente și avertizări de securitate.

Utilizați un sistem Managementul evenimentelor și informațiilor de securitate (SIEM) pentru a agrega și a corela datele astfel încât să detectați mai bine activități și modele suspecte care indică posibile intruziuni în rețea și evenimente, cum ar fi acreditări divulgate, adrese IP eronate și accesul de pe dispozitive infectate.

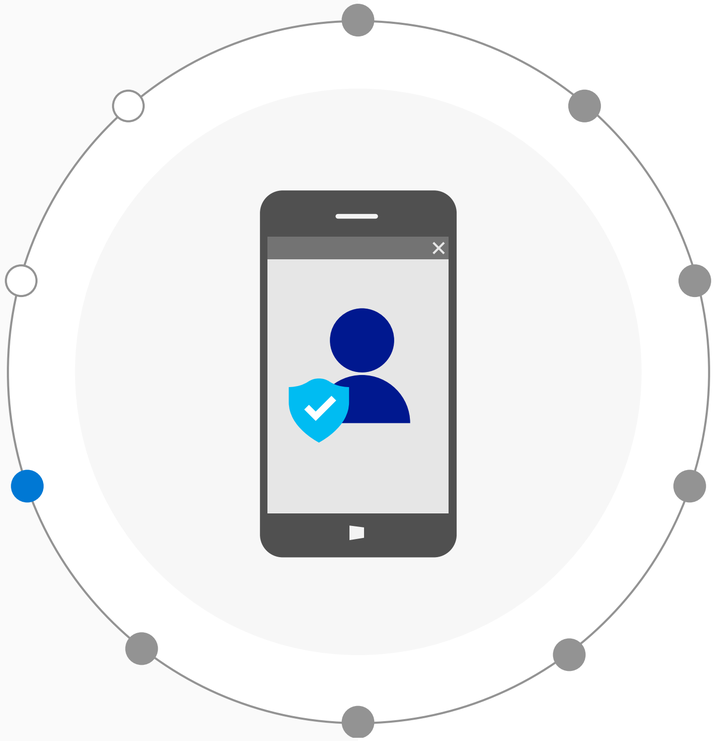


Un sistem SIEM poate fi utilizat pentru a efectua auditarea activității utilizatorului, a documenta conformitatea cu cerințele de reglementare și a ajuta la o analiză judiciară.

De asemenea, poate îmbunătăți monitorizarea accesului cel mai puțin privilegiat și poate garanta că utilizatorii au acces numai la resursele de care au cu adevărat nevoie.

Sfat 08

Activați auto-asistența utilizatorului final



Este posibil ca utilizatorii să fie mult mai puțin refractari la Zero Trust decât la multe alte inițiative de securitate.

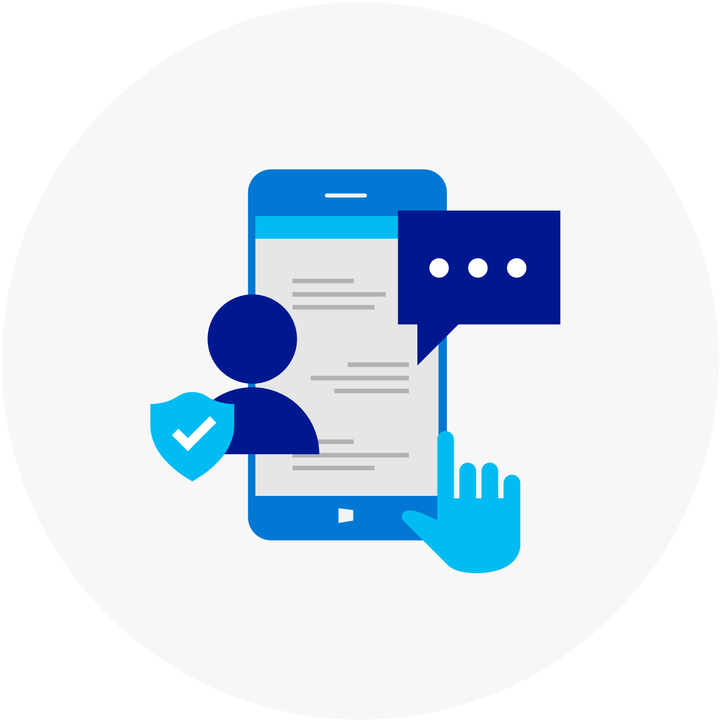
Motivul este că sunt deja familiarizați cu accesul pe baza identității pe dispozitivele și aplicațiile personale și doresc aceeași experiență la locul de muncă. Zero Trust permite organizațiilor de securitate să securizeze (și să spună afirmativ la) scenarii de productivitate moderne, cum ar fi dispozitive mobile, BYOD și aplicații SaaS, pentru a păstra nivelul de satisfacție a utilizatorilor fără a compromite securitatea.

Sfat 08

Activați auto-asistența utilizatorului final

Este posibil ca utilizatorii să fie mult mai puțin refractari la Zero Trust decât la multe alte inițiative de securitate.

Motivul este că sunt deja familiarizați cu accesul pe baza identității pe dispozitivele și aplicațiile personale și doresc aceeași experiență la locul de muncă. Zero Trust permite organizațiilor de securitate să securizeze (și să spună afirmativ la) scenarii de productivitate moderne, cum ar fi dispozitive mobile, BYOD și aplicații SaaS, pentru a păstra nivelul de satisfacție a utilizatorilor fără a compromite securitatea.



Echipele IT pot reduce fricțiunile, permițându-le utilizatorilor să efectueze anumite activități de securitate, cum ar fi resetările neasistate ale parolelor.

Faptul de a le permite utilizatorilor să-și reseteze sau să-și deblocheze parolele de cont fără implicarea administratorului, monitorizându-se totodată eventualele abuzuri sau utilizări incorecte, asigură un echilibru eficient între securitate și productivitate.

În mod similar, implementarea gestionării grupului cu autoservire le permite proprietarilor să creeze și să gestioneze grupuri fără a fi necesar ca un administrator să facă acest lucru.

Sfat 09

Nu exagerați cu promisiunile



Zero Trust nu este o inițiativă „big bang” unică, precum implementarea autentificării multi-factor.

Aceasta vizează o etapă finală de lungă durată cu o nouă generație de controale de securitate construite complet diferit de modelele tradiționale de acces bazate pe rețea.

Sfat 09

Nu exagerați cu promisiunile

Zero Trust nu este o inițiativă „big bang” unică, precum implementarea autentificării multi-factor.

Aceasta vizează o etapă finală de lungă durată cu o nouă generație de controale de securitate construite complet diferit de modelele tradiționale de acces bazate pe rețea.



Aplicarea acestei viziuni necesită timp și un set permanent de proiecte mai mici.

Pe parcurs, este important să stabiliți și să gestionați în mod corespunzător așteptările. Acceptați suportul participanților direct interesați și concepeți un plan de comunicare eficientă cu aceștia pe parcursul ciclului de viață al proiectului. Pregătiți-vă să luați măsuri pentru a depăși rezistența culturală și alte provocări din partea unor grupuri obișnuite de multă vreme să facă lucrurile cu totul altfel.

Sfat 10

Prezentați valoare pe parcurs



Una dintre cele mai eficiente modalități de a construi o susținere pe termen lung pentru o inițiativă Zero Trust este să demonstrați o valoare incrementală cu fiecare investiție.

În cadrul anchetei de securitate desfășurată de IDG, mai mult de jumătate din respondenți (51%) au spus că un model de acces Zero Trust ar contribui la îmbunătățirea capacității de protejare a datelor clienților, iar 46% au afirmat că acesta ar ajuta la activarea unei experiențe superioare și mai sigure pentru utilizatorul final.

Sfat 10

Prezentați valoare pe parcurs

Una dintre cele mai eficiente modalități de a construi o susținere pe termen lung pentru o inițiativă Zero Trust este să demonstrați o valoare incrementală cu fiecare investiție.

În cadrul anchetei de securitate desfășurată de IDG, mai mult de jumătate din respondenți (51%) au spus că un model de acces Zero Trust ar contribui la îmbunătățirea capacității de protejare a datelor clienților, iar 46% au afirmat că acesta ar ajuta la activarea unei experiențe superioare și mai sigure pentru utilizatorul final.



Capacitatea dvs. de a lua decizii bune privind controlul accesului depinde de calitatea, cantitatea și diversitatea semnalelor pe care le integrați în acele decizii.

De exemplu, integrarea unor surse de investigare a amenințărilor, cum ar fi adrese IP pentru programe bot sau malware, va forța adversarii să obțină în permanență resurse noi. Integrarea mai multor detalii despre conectare (oră, locație etc.) urmărind apoi dacă aceasta corespunde cu rutina normală a utilizatorului va fi mai greu de imitat pentru atacatori, reducând în același timp neplăcerile utilizatorului.

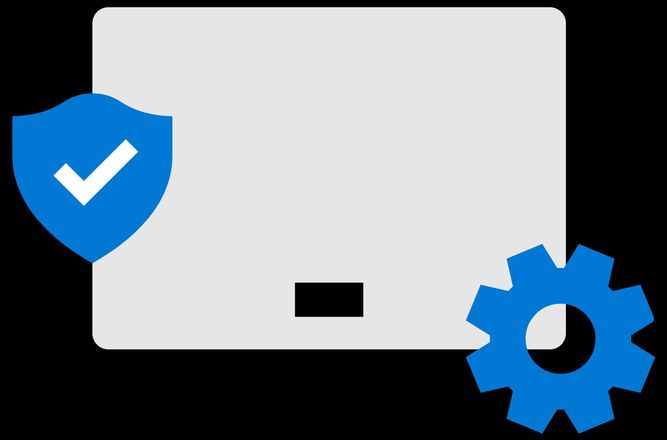
Microsoft 365

Un model pentru viitor

Nu avem cum să prevedem ce exploatări noi vor apărea la un moment dat și cum ar putea obține intrarea în mediul dvs. Pentru că nimeni nu poate garanta că un anumit utilizator sau dispozitivul, aplicația sau rețeaua pe care le utilizează este complet sigur, singura abordare rezonabilă a securității este să nu aveți încredere în nimic și să verificați totul.

Un model Zero Trust nu este ușor de obținut, dar este un element esențial al oricărui obiectiv de modernizare pe termen lung pentru întreprinderea digitală.

Pentru a afla mai multe despre cum să abordați direct provocările privind securitatea cibernetică:



Vizitați Seria noastră Microsoft CISO Spotlight

[1] Anchetă IDG Explorer, mai 2019
[2] Studiul Priorități de securitate IDG, 2018, https://www.idg.com/tools-for-marketers/2018-security-priorities-study/
[3] Wikipedia, https://en.wikipedia.org/wiki/Jericho_Forum
[4] CSO, July 2018, https://www.csoonline.com/article/3287057/what-it-takes-to-build-a-zero-trust-network.html

©2019 Microsoft Corporation. Toate drepturile rezervate. Acest document este furnizat „ca atare”. Informațiile și opiniile exprimate în acest document, inclusiv URL-ul și alte referințe la site-uri web, se pot modifica fără notificare prealabilă. Vă asumați riscul utilizării acestuia. Acest document nu vă oferă drepturi legale pentru nicio proprietate intelectuală dintr-un produs Microsoft. Puteți să copiați și să utilizați acest document pentru scopuri interne, de referință.