
Ești pregătit să faci față
UNUI ATAC CIBERNETIC?
vodafone business
Microsoft Solutions Partner
Modern Work

Într-o lume digitală în continuă mișcare, în care atacurile cibernetice devin tot mai sofisticate, afacerile mici nu mai pot ignora realitatea: riscurile sunt reale și cresc în fiecare zi. Studiile recente realizate de Microsoft și Allianz confirmă acest lucru – securitatea cibernetică nu mai este un lux, ci o necesitate critică pentru supraviețuirea și succesul oricărei companii, indiferent de dimensiune.

Dar de ce rămân IMM-urile vulnerabile?

Un **studiu Microsoft** din septembrie 2024 a semnalat percepțiile greșite care le mențin în zona de risc:

44%
cred că dacă au fost deja atacați, nu vor mai fi vizați.

26%
presupun că, nefiind atacați până acum, sunt în siguranță.

26%
consideră că sunt prea mici pentru a atrage atenția hackerilor.

vodafone business

Microsoft Solutions Partner
Modern Work

Și totuși, realitatea este alta la nivelul afacerilor mici. Barometrul de Risc Allianz 2025 arată că incidentele cibernetice sunt percepute drept cel mai mare risc global – cu un procent de 38% în 2025, o creștere semnificativă față de acum zece ani, când ocupau doar locul 8 cu 12%.

Responsabilii din departamentele de IT ale IMM-urilor știu că riscurile cresc și încearcă să rămână informați și pregătiți pentru astfel de atacuri. Și totuși, când vine vorba de bugete, securitatea rămâne de multe ori pe lista de „mai vedem”. De ce? Pentru că realitatea este că aceste companii au mai puține resurse, mai puține instrumente și mai puțină expertiză tehnică internă decât companiile mari.

Dar atacurile nu țin cont de dimensiune. Un singur incident poate însemna:

1. 

Pierderi financiare greu de recuperat

2. 

Afectarea reputației în fața clienților și partenerilor

3. 

Blocaje în activitate care paralizează productivitatea

*Barometrul de Risc Allianz, ediția a 14-a, încorporează opiniile a 3.778 de respondenți din 106 țări și teritorii. Respondenții au fost chestionați în perioada octombrie-noiembrie 2024, iar sondajul s-a concentrat pe companii mari (46%), mici (29%) și mijlocii (25%). Iată care sunt Top 5 riscuri identificate de organizații. Pentru top 10 puteți consulta Barometrul **aici.** **Anexa pe țări.**

SECURITATEA DIGITALĂ NU MAI ESTE DOAR O SOLUȚIE PENTRU AFACEREA TA:

1 din 3 IMM-uri a fost victima unui atac cibernetic*

Problema

31% dintre IMM-uri au fost victimele atacurilor cibernetice de tip ransomware, phishing sau breșe de date; astfel riscurile sunt ridicate indiferent de mărimea companiei.

Soluție

Iată patru bune practici simple pentru a crea o fundație solidă de securitate cibernetică.

1. Folosește parole puternice și ia în considerare utilizarea unui manager de parole.
2. Activează autentificarea multifactor.
3. Învață să recunoști și să raportezi phishing-ul.
4. Asigură-te că software-ul este actualizat

Atacurile cibernetice costă IMM-urile mai mult de 250.000 $ în medie și până la 7.000.000 $*

Problema

Costurile ascunse ale unui atac cibernetic pot destabiliza complet un IMM. De la investigații și recuperare, până la amenzi pentru breșe de date, impactul financiar este adesea copleșitor. Mai mult, încrederea clienților poate fi afectată pe termen lung, ducând la pierderi de reputație și oportunități de afaceri. Deși multe IMM-uri sunt optimiste în privința rezilienței lor, realitatea este că recuperarea poate dura de la o zi la peste o lună – un interval greu de anticipat fără o strategie solidă de securitate.

Soluție

Evaluare și planificare

1. Efectuează o **evaluare a riscurilor de securitate cibernetică** pentru a înțelege lacunele în securitate și pentru a determina pașii necesari pentru a le rezolva. Evaluările te ajută să descoperi zonele vulnerabile la atacuri din afacerea ta, pentru a le minimiza; să asiguri conformitatea cu cerințele de reglementare; să stabilești planuri de răspuns la incidente și multe altele.
2. **Planifică eficient și proactiv**. Poți minimiza costurile financiare, de reputație și operaționale asociate cu un atac cibernetic, în cazul în care acesta ar avea loc. Multe organizații oferă auto-evaluări, iar colaborarea cu un specialist în securitate sau un furnizor de servicii de securitate poate aduce expertiză și îndrumare suplimentară pe parcursul procesului, după cum este necesar.

vodafone business

Microsoft Solutions Partner
Modern Work

81% dintre IMM-uri cred că inteligența artificială crește necesitatea unor controale suplimentare de securitate*

Problema

Progresul rapid al tehnologiilor AI și ușurința de utilizare prin interfețe simple creează provocări notabile pentru IMM-uri atunci când sunt utilizate de angajați. Fără instrumentele adecvate pentru a securiza datele companiei, utilizarea AI poate duce la expunerea informațiilor sensibile sau confidențiale în medii greșite. Din fericire, mai mult de jumătate dintre companiile care nu folosesc în prezent instrumente de securitate AI intenționează să le implementeze în următoarele șase luni pentru o securitate mai avansată.

Soluție

Ai grijă de securitatea și guvernanța datelor

Pentru ca inteligența artificială să fie adoptată și utilizată cu succes în cadrul unei organizații, este esențial să existe un cadru solid de securitate și guvernanță a datelor. Prin aplicarea unor măsuri precum etichetarea și criptarea documentelor, companiile pot preveni ca informațiile sensibile să fie accesate sau utilizate necorespunzător de sistemele AI. În paralel, implementarea unei strategii clare de guvernanță a datelor — care presupune gestionarea, clasificarea și protejarea acestora — oferă o bază sigură și organizată pentru dezvoltarea responsabilă a soluțiilor bazate pe inteligență artificială.

94% consideră că securitatea cibernetică este esențială pentru afacerea lor*

Problema

Resurse și expertiză limitate.

Recunoscând importanța critică a securității cibernetice, 94% dintre IMM-uri o consideră esențială pentru operațiunile lor. Deși nu a fost întotdeauna considerată o prioritate de top, având în vedere resursele limitate și expertiza internă, creșterea amenințărilor cibernetice și sofisticarea tot mai mare a atacurilor cibernetice reprezintă acum riscuri semnificative pentru IMM-uri. Gestionarea datelor de lucru pe dispozitive personale, ransomware-ul și phishing-ul sunt citate ca principale provocări cu care se confruntă IMM-urile.

Soluție

Chiar dacă nu ai o echipă IT dedicată sau ai o echipă IT mică; chiar dacă nu ai bugete mari, poți face pași concreți pentru a-ți proteja afacerea. O soluție accesibilă este instruirea angajaților prin resurse gratuite și ușor de înțeles, precum cele oferite de Microsoft prin **platforma de Conștientizare a Securității Cibernetice**.

Aici poți găsi materiale utile despre subiecte esențiale precum Cybersecurity 101, recunoașterea tentativelor de phishing și bune practici de protejare a datelor.

vodafone business

Microsoft Solutions Partner
Modern Work

Mai puțin de 30% dintre IMM-uri își gestionează securitatea intern*

Problema

Având în vedere resursele limitate și expertiza internă din cadrul IMM-urilor, multe dintre acestea apelează la specialiști în securitate pentru asistență. Mai puțin de 30% dintre IMM-uri își gestionează securitatea intern și, în general, se bazează pe consultanți de securitate sau furnizori de servicii pentru a-și gestiona nevoile de securitate. Acești profesioniști în securitate oferă suport crucial în cercetarea, selectarea și implementarea soluțiilor de securitate cibernetică; asigurându-se că IMM-urile sunt protejate împotriva noilor amenințări.

Soluție

Apelează la expertiza unui furnizor de servicii gestionate (Managed Services)

Colaborarea cu un furnizor de servicii IT gestionate este o soluție eficientă pentru IMM-urile cu resurse limitate. Acești furnizori identifică, implementează și gestionează soluții de securitate adaptate nevoilor afacerii tale. Un astfel de furnizor suntem și noi. Vodafone Business este aici să fie partenerul tău de tehnologie. Noi îți gestionăm aplicațiile, iar tu și echipa ta vă concentrați pe obiectivele de business.

Află mai multe despre Managed Services pentru Microsoft 365.

80% intenționează să își mărească cheltuielile pentru securitatea cibernetică, cu protecția datelor ca principală zonă de cheltuieli*

Problema

Majoritatea IMM-urilor recunosc riscurile tot mai mari și intenționează să crească bugetele pentru securitate cibernetică, în special pentru protecția datelor — unul dintre principalii factori motivaționali sunt protecția împotriva pierderilor financiare și protejarea datelor clienților și ale utilizatorilor.

Soluție

Alege să investești în protecția datelor:

1. Soluții precum Prevenirea Pierderii Datelor (DLP) te ajută să identifici activități suspecte și să previi scurgerea informațiilor sensibile din afacerea ta.
2. Cu ajutorul tehnologiilor de tip EDR (Detectare și Răspuns la Endpoint), îți poți proteja dispozitivele, iar prin IAM (Gestionarea Identității și Accesului), te asiguri că doar persoanele potrivite au acces la datele corecte.
3. Alte domenii principale de cheltuieli includ servicii de firewall, protecția împotriva phishing-ului, protecția împotriva ransomware-ului și a dispozitivelor, controlul accesului și gestionarea identității.

vodafone business

Microsoft Solutions Partner
Modern Work

68% dintre IMM-uri consideră accesul securizat la date o provocare pentru lucrătorii la distanță*

Problema

68% dintre IMM-uri consideră dificilă asigurarea accesului securizat la date pentru angajații care lucrează de la distanță, mai ales în contextul muncii hibride. Riscul pierderii datelor pe dispozitive personale este o preocupare majoră.

Soluție

Implementarea unor soluții de securitate și gestionare a dispozitivelor pentru a proteja informațiile sensibile într-un mediu de lucru hibrid. Actualizări automate, aplicații sigure și politici clare de partajare a datelor ajută IMM-urile ca informațiile sensibile să fie în siguranță și să ofere angajaților un mediu de lucru sigur, indiferent de locație.

*Conform raportului Microsoft referitor la securitatea cibernetică

DE LA RISC LA PROTECȚIE: CUM ÎNCEPE UN PLAN DE SECURITATE EFICIENT

Ca antreprenor, știi cât de greu este să găsești echilibrul între modernizare, susținerea echipei și protejarea afacerii tale. Dar securitatea cibernetică nu mai poate fi lăsată pe plan secund. Ai nevoie să securizezi accesul la e-mailuri și fișiere, să protejezi datele în timp ce colaborezi eficient, să te ferești de phishing, spam și malware, dar și să îți păzești dispozitivele mobile.

Vestea bună? Nu ești singur. Aproape 80% dintre liderii de afaceri spun că vor crește bugetele pentru securitate cibernetică.
Ce îi motivează?

60%

vor să își protejeze compania de pierderi financiare.

56%

vor să asigure confidențialitatea datelor clienților.

vodafone business

Microsoft Solutions Partner
Modern Work

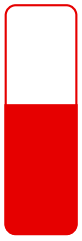
Unde își vor concentra IMM-urile cheltuielile?

65%

pentru creșterea protecției datelor

54%

pentru firewall și/sau firewall ca serviciu

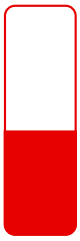


53%

pentru protecția împotriva phishing-ului

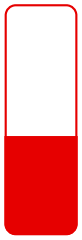
52%

pentru protecția împotriva ransomware-ului și protecția dispozitivelor



46%

pentru controlul accesului și gestionarea identității



45%

pentru gestionarea dispozitivelor

44%

pentru serviciul de detectare și răspuns gestionat

34%

pentru gestionarea patch-urilor

vodafone business

Microsoft Solutions Partner
Modern Work

LA CE MAI POȚI FI ATENT PENTRU A-ȚI PĂSTRA AFACEREA ÎN SIGURANȚĂ

Ajută pe toată lumea din organizația ta să înțeleagă ce poate face pentru a se menține pe sine și pe colegi în siguranță online, urmând aceste bune practici.

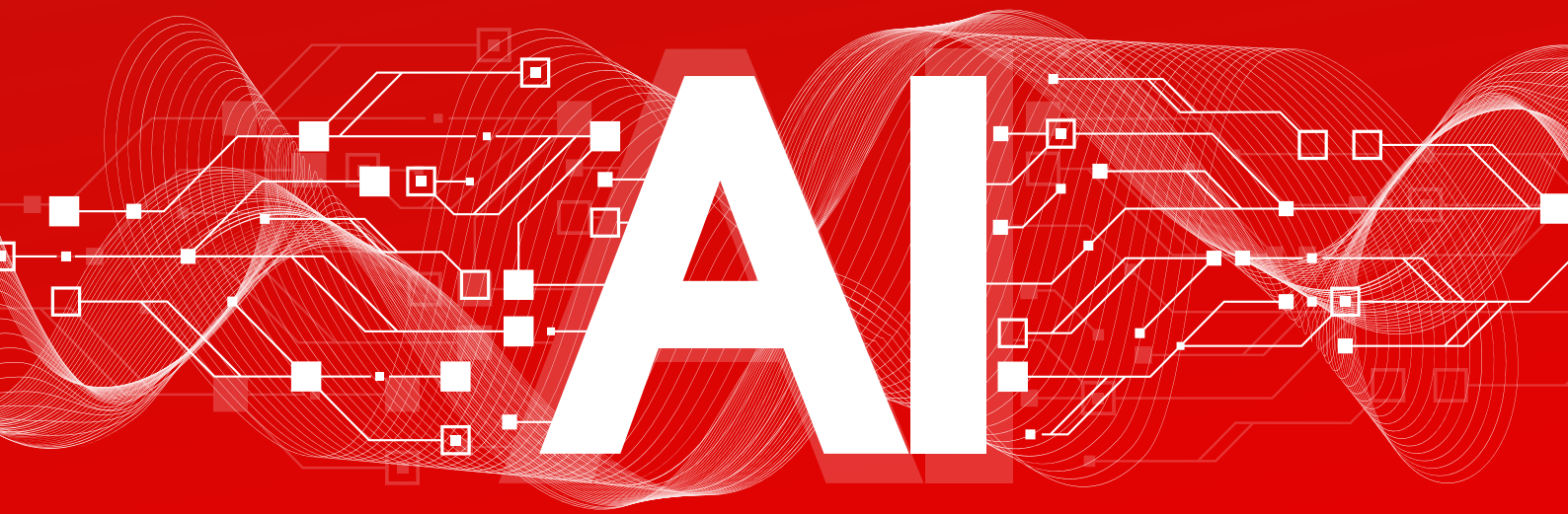
CUM FOLOSEȘTI AI-UL ÎN SIGURANȚĂ ÎN AFACEREA TA

Inteligența artificială generativă poate crește productivitatea; dar vine cu riscuri precum:

- **Supradependența** - acceptarea rezultatelor AI ca fiind autoritare te poate face să iei decizii greșite. AI-urile nu sunt motoare de căutare; astfel poți primi informații greșite.
- **Impersonarea** - Poate fi folosită pentru a imita colegi sau superiori (ex: cereri false de plată).
- **Manipularea socială generată de AI** - Poate genera conținut manipulator (ex: conturi false, articole părtinitoare). Această tactică este folosită pentru tot - de la fraudă și spionaj industrial până la operațiuni de influență cibernetică.

Ce poți face concret pentru afacerea ta

- Alege doar soluții AI aprobate de echipa IT.
- Protejează datele sensibile de utilizarea AI-ului prin criptare și etichetare.
- Dă-i sarcini clare AI-ului și verifică rezultatele.



vodafone business

Microsoft Solutions Partner
Modern Work

CYBERSECURITY 101

IMM-urile sunt tot mai expuse atacurilor cibernetice, fie prin rețea (ex: atacuri DoS/DDoS), fie prin manipularea angajaților (ex: phishing, vishing, smishing). Lipsa unor măsuri de bază poate duce la pierderi de date, bani și încredere.

Care sunt cele mai frecvente tipuri de atacuri cibernetice?

La nivel de rețea:

- **Denial of service (DoS)**: Un atac în care un computer trimite multe solicitări către un serviciu de rețea pentru a copleși serviciul țintă.
- **Distributed denial of service (DDoS)**: Similar cu un atac DoS, doar că folosește mai multe computere în mai multe locații într-un atac coordonat.

Ce vizează oamenii:

- **Phishing și spear phishing**: e-mailuri primite ce par a fi de la un coleg, prieten,o persoană sau companie de încredere, conținând un link sau un atașament.
- **Vishing**: Similar cu phishing-ul, dar folosind apeluri telefonice în loc de e-mailuri.
- **Smishing**: Similar cu phishing-ul, dar folosind mesaje text SMS în loc de e-mailuri.
- **Baiting**: Atunci când atacatorul tentează cu un premiu fals sau o ofertă pentru a răspunde la un atac de phishing sau vishing.
- **Atacuri de browser**: Aceste atacuri pot apărea sub formă de reclame pop-up sau sugestii de instalare a unei extensii de browser.

Protejează-ți afacerea cu măsuri simple și eficiente:

- Oferă training de securitate cibernetică angajaților și simularea atacurilor în Microsoft Defender pentru Office 365
- Activează autentificarea multi-factor și evită parolele slabe.
- Folosește soluții precum Microsoft Defender și actualizează constant sistemele.
- Impune protocoale de salvare a fișierelor, criptează datele și stochează-le în Cloud.
- Blochează pop-up-urile și folosește extensii de securitate în browser.

vodafone business

Microsoft Solutions Partner
Modern Work

PROTEJAREA DISPOZITIVELOR

Fie că lucrezi de la birou sau de pe telefon, obiceiurile nesigure pot pune în pericol datele companiei. Linkuri suspecte, parole slabe sau aplicații neoficiale sunt doar câteva dintre riscuri.

Adoptă câțiva pași simpli pentru o securitate digitală solidă:

1. **Nu te încrede în linkuri din mesaje suspecte.**

Dacă ți se cer date personale, caută direct pe site-ul oficial un număr de contact și verifică autenticitatea mesajului.

2. **Nu deschide fișiere atașate neașteptate.**

Chiar dacă par să vină de la persoane cunoscute, verifică dacă chiar ei sunt expeditorii.

3. **Trimite informații personale doar în timp real.**

Evită e-mailurile sau mesajele pentru date sensibile. Dacă e absolut necesar, criptează datele.

4. **Renunță la parole.**

Activează autentificarea fără parolă cu telefonul sau Windows Hello pentru mai multă siguranță.

5. **Dacă totuși folosești parole, creează unele puternice și unice.**

Un manager de parole și Microsoft Edge te pot ajuta să le gestionezi.

6. **Instalează actualizările software imediat**

și asigură-te că instalezi aplicații doar din magazinele oficiale.

7. **Activează Protecția împotriva modificărilor neautorizate în Windows 11.**

Astfel, setările tale de securitate rămân protejate.8. Scanează firmware-ul periodic. Astfel, identifici vulnerabilitățile din sistem.

8. **Scanează firmware-ul periodic.**

Astfel identifici vulnerabilitățile din sistem.

9. **Redu suprafața de atac.**

Elimină conexiunile inutile la internet, restricționează porturile deschise și folosește instrumente de scanare pentru a verifica mediul digital în căutarea punctelor slabe.

vodafone business

Microsoft Solutions Partner
Modern Work

FRAUDĂ

Escrocheriile de tip „suport tehnic” devin tot mai sofisticate. Atacatorii se dau drept tehnicieni și încearcă să obțină acces la date sau bani prin apeluri, mesaje sau aplicații false.

Ce abordări există pentru o astfel de fraudă:

1. **Primești un apel neașteptat de la „suport tehnic”.**

Microsoft și Vodafone nu te sună din senin. Dacă nu ai cerut ajutor, ignoră apelul.

2. **Vezi un mesaj de eroare care îți cere să suni urgent.**

Mesajele Microsoft nu includ numere de telefon. Edge blochează automat site-urile suspecte.

3. **Ți se cere să plătești cu criptomonede sau carduri cadou.**

Niciun tehnician serios nu cere astfel de plăți. Costurile reale sunt comunicate clar, în avans.

4. **Ești rugat să descarci software dintr-un e-mail sau site necunoscut.**

Descarcă doar din surse oficiale – site-ul Microsoft sau magazinele de aplicații.

5. **Ți se cere parola sau alte date personale.**

Suportul tehnic legitim nu îți va cere niciodată astfel de informații.

Ce poți face dacă ai fost fraudat?

- Dezinstalează aplicațiile suspecte și rulează o scanare completă.
- Schimbă parolele și resetează dispozitivul dacă a fost accesat.
- Contactează banca dacă ai făcut o plată.
- Raportează frauda pe **https://www.microsoft.com/reportascam**
- Activează soluții de securitate (ex: EDR) și limitează privilegiile și accesul angajaților la strictul necesar.
- Raportează site-urile suspecte în Microsoft Edge: Setări > Ajutor și feedback > Raportează site nesigur.

vodafone business

Microsoft Solutions Partner
Modern Work

PHISHING

Phishing-ul este o metodă frecventă de fraudă digitală prin care atacatorii încearcă să obțină date sensibile, folosind e-mailuri, linkuri sau coduri QR false care par legitime.

Tipuri de phishing:

1. Injectarea de conținut

Un site cunoscut (ex: bancă, e-mail) este modificat cu un formular sau pop-up fals care îți cere date personale.

2. Manipularea linkurilor

Primești un link care pare de încredere, dar te duce pe un site fals unde ți se cer datele de autentificare.

3. E-mailuri

Mesaje care par legitime, dar conțin linkuri, atașamente sau coduri QR periculoase. Ținta? Să-ți fure datele sau să instaleze malware.

4. Atacuri de tip „omul din mijloc”

Un atacator interceptează comunicarea dintre tine și altcineva, modificând sau furând informații.

5. Coduri QR malițioase

Un cod QR dintr-un e-mail sau afiș poate duce către un site fals sau poate instala aplicații dăunătoare pe telefon.

Protejează-ți afacerea cu câteva reguli simple:

Nu accesa linkuri sau coduri QR din surse nesigure.

Nu deschide atașamente neașteptate, chiar dacă par de la cunoscuți.

Autentifică-te doar din site-ul oficial, nu din linkuri primite.

Activează filtrele anti-phishing și anti-spam din e-mail.

Fii sceptic cu orice mesaj care cere date personale sau autentificare rapidă.

vodafone business

Microsoft Solutions Partner
Modern Work

SECURIZAREA PROCESULUI DE AUTENTIFICARE

Parolele slabe și lipsa autentificării suplimentare pot compromite rapid conturile și datele companiei. Multe atacuri cibernetice încep cu o autentificare neprotejată. Iată câteva recomandări pentru cum poți avea o parolă mai puternică:

1. Creează parole inteligente:

Pentru administratori:

- Cere parole de minim 8 caractere
- Evită cerințele specifice privind compoziția caracterelor (de ex., *&(^%$).
- Nu forța resetări periodice
- Blochează parolele comune
- Încurajează utilizatorii să nu refolosească parolele în scop personal

Pentru utilizatori:

- Nu folosi aceeași parolă pe mai multe site-uri
- Evită parole simple sau expresii populare
- Creează parole greu de ghicit, fără nume sau date personale

2. Folosirea MFA reduce cu peste 99% riscul de compromitere a contului.

- Impune înregistrarea MFA (autentificarea multifactor)
- Activează provocările bazate pe risc

3. Autentificarea fără parolă e mai sigură și mai simplă. Folosește:

- Windows Hello
- Chei de securitate FIDO2
- Passkey-uri

vodafone business

Microsoft Solutions Partner
Modern Work

CONCLUZIE

IMM-urile agile conștientizează tot mai mult importanța protejării datelor sensibile – fie că este vorba despre informații interne, date ale clienților sau alte active digitale esențiale. Într-un peisaj digital în continuă schimbare, în care amenințările cibernetice devin tot mai sofisticate, aceste companii adoptă o abordare proactivă pentru a-și consolida securitatea. Implementarea unor instrumente moderne de protecție, alături de expertiza tehnică necesară pentru a detecta și preveni atacurile, nu mai este doar o opțiune, ci un diferențiator strategic.

Succesul nu mai este definit doar de agilitate operațională, ci și de capacitatea de a construi un ecosistem digital sigur și rezilient. De aceea, IMM-urile care investesc în soluții de securitate scalabile și ușor de integrat în infrastructura existentă își sporesc nu doar protecția, ci și încrederea clienților și a partenerilor. În plus, colaborarea cu furnizori de încredere și adoptarea celor mai bune practici, în materie de conformitate și protecție a datelor, devin piloni esențiali în strategia de creștere sustenabilă.

Vodafone Business este partenerul tău de tehnologie, în acest demers. În calitate de partener global Microsoft, ne-am angajat să susținem IMM-urile în extinderea capabilităților tehnologice și consolidarea securității cibernetice.

Oferim pachete dedicate, cu costuri optimizate, care îmbină simplitatea implementării cu eficiența protecției.

Contactează specialistul de cont pentru a discuta despre Soluțiile de Securitate Microsoft.

Surse:

Secure Our World—Together

SMBCybersecurity-Report-Final.pdf

Risk Barometer

Risk Barometer – anexa pe țări

vodafone business

Microsoft Solutions Partner
Modern Work