Shadow IT: Najväčšie bezpečnostné riziko, o ktorom väčšina majiteľov firiem nevie

29.6.2026 - | COMTEC s. r. o.

Predstavte si, že sa spýtate svojich zamestnancov jednoduchú otázku: „Aké aplikácie používate počas pracovného dňa?“ Väčšina majiteľov firiem očakáva odpoveď typu Microsoft 365, Outlook alebo firemné CRM. Realita je často úplne iná.

Čo sa v článku dozviete

- · Čo je Shadow IT a prečo je dnes väčším problémom ako kedykoľvek predtým
- · Ako vzniká Shadow AI – nová kategória rizika, ktorú väčšina firiem ešte nepozná
- · Prečo zákaz AI nástrojov problém nevyrieši
- · 5 najčastejších príkladov Shadow IT v slovenských firmách
- · Rýchly 10-minútový audit, ktorý zistí, či má vaša firma problém
- · Ako Shadow IT dostať pod kontrolu – bez zákazov, ktoré nikto nedodrží

Zamestnanci si pomáhajú vlastnými nástrojmi. Posielajú dokumenty cez osobný Google Disk, komunikujú cez WhatsApp, používajú vlastné ChatGPT účty alebo si ukladajú firemné súbory do Dropboxu. Dôvodom býva najmä to, že jednoducho chcú pracovať rýchlejšie.

Práve toto sa nazýva **Shadow IT** – technológie používané bez vedomia alebo schválenia IT oddelenia. A v poslednom období pribudol nový problém: **Shadow AI**.

Nejde o hackerský útok. Ide o bežný pracovný deň.

Čo je Shadow IT?

Shadow IT označuje akýkoľvek softvér, cloudovú službu alebo zariadenie, ktoré zamestnanci používajú pri práci bez schválenia firmy alebo IT oddelenia.

Pred niekoľkými rokmi išlo najmä o Dropbox, osobný Gmail, vlastné USB kľúče alebo neoficiálne cloudové úložiská. Dnes sa zoznam výrazne rozšíril. Najčastejšie ide o:

ChatGPTGeminiClaudeOsobný Google DiskWhatsAppSignalWeTransferBezplatné AI nástroje

Prečo zamestnanci používajú Shadow IT?

Vo väčšine prípadov nejde o úmyselné porušenie pravidiel. Dôvody sú úplne praktické:

- · potrebujú rýchlo zdieľať veľký súbor
- · chcú si uľahčiť písanie e-mailov pomocou AI
- · firemné riešenia sú pomalé
- · nevedia, že existuje schválená alternatíva
- · nikto im nikdy nevysvetlil riziká

Shadow AI – nový problém, ktorý rastie najrýchlejšie

Najrýchlejšie rastúcou kategóriou Shadow IT je dnes používanie generatívnej umelej inteligencie.

Typický scenár vyzerá takto: Marketingový pracovník vloží do ChatGPT:

„Priprav cenovú ponuku pre spoločnosť XY.“

Do promptu skopíruje:

obchodnú ponukucenykontaktné údaje zákazníkainterné procesy

Za niekoľko sekúnd získava kvalitný text. Zároveň však firma často vôbec netuší, že citlivé údaje boli odoslané mimo jej kontrolovaného prostredia.

 Čo na to hovoria bezpečnostné rámce Bezpečnostné rámce vrátane odporúčaní **NIST** a **ENISA** upozorňujú, že organizácie majú zaviesť správu AI nástrojov namiesto ich nekontrolovaného používania. Bez pravidiel môže dôjsť k úniku obchodného tajomstva alebo osobných údajov.

Cesta firemných dát: čo sa stane, keď zamestnanec použije osobný ChatGPT

Aby ste videli, prečo je toto riziko skutočné a nie teoretické, tu je presná cesta, akou sa dáta pohybujú:

 Bez firemných pravidiel

Zamestnanec kopíruje dáta do promptu
→
Osobný účet (ChatGPT, Gemini…)
→
Server tretej strany (iná jurisdikcia)
→
Dáta mimo kontroly firmy

 S firemným riešením

Zamestnanec pracuje s dátami
→
Schválený podnikový nástroj
→
Kontrolované prostredie firmy
→
Auditovateľný prístup

Rozdiel medzi týmito dvoma cestami je presne to, čo oddeľuje firmu, ktorá má dáta pod kontrolou, od firmy, ktorá to zistí až pri incidente alebo audite.

5 najčastejších príkladov Shadow IT v slovenských firmách

1**Osobný Google Disk**
Zamestnanec potrebuje pracovať z domu. Firemné dokumenty si jednoducho presunie na svoj súkromný účet. Ak odíde z firmy, dokumenty zostávajú u neho.
2**ChatGPT alebo iné AI nástroje**
Do AI sa často kopírujú zmluvy, cenové ponuky, databázy zákazníkov, zdrojové kódy aj interné smernice. Mnohí používatelia si neuvedomujú, že nie každý AI nástroj poskytuje rovnaké podnikové garancie ochrany dát.
3**WhatsApp komunikácia**
Obchodníci si vytvoria vlastnú skupinu. Posielajú si cenové ponuky, fotografie projektov, kontakty zákazníkov, faktúry. Po odchode zamestnanca firma často stratí prehľad o celej komunikácii.
4**WeTransfer alebo bezplatné úložiská**
Veľké súbory sa odosielajú mimo firemných systémov. Nikto nevie, kto ich otvoril, kde skončili, ako dlho budú dostupné.
5**Vlastné AI rozšírenia do prehliadača**
Dnes existujú stovky AI doplnkov. Niektoré automaticky čítajú e-maily, dokumenty, obsah webových stránok. Ak nie sú schválené IT oddelením, predstavujú ďalší nekontrolovaný kanál pre firemné dáta.

Prečo je Shadow IT také nebezpečné?

Najväčší problém nie je samotný nástroj. **Problémom je strata kontroly.**

Firma nevie:

- □ kde sa nachádzajú jej dáta
- □ kto k nim má prístup
- □ či sú šifrované
- □ či sa zálohujú
- □ či spĺňajú požiadavky GDPR alebo NIS2

To môže mať následky nielen pri kybernetickom incidente, ale aj počas auditu alebo riešenia bezpečnostného incidentu – v momente, keď je odpoveď na tieto otázky najpotrebnejšia.

Krátky mini audit: Má vaša firma problém so Shadow IT?

Odpovedzte si na tieto otázky – stačí pravdivo, nie dokonale:

Vie váš tím presne povedať, ktoré cloudové úložiská firma oficiálne používa?
Existuje pravidlo, ktorý AI nástroj sa môže a nesmie používať pri práci s citlivými dátami?
Viete, či zamestnanci komunikujú s klientmi cez WhatsApp alebo Signal?
Máte prehľad, kam smerujú súbory odoslané cez WeTransfer alebo podobné služby?
Pri odchode zamestnanca viete s istotou, že firemné dáta nezostali na jeho osobných účtoch?
Vedia zamestnanci, prečo je kopírovanie firemných dát do verejného ChatGPT rizikové?

Vyhodnotenie

Ak ste odpovedali „nie“ alebo „nie som si istý“ na **2 a viac otázok**, vaša firma má pravdepodobne aktívny Shadow IT problém – len o ňom ešte nevie.

Ako dostať Shadow IT pod kontrolu

Najväčšou chybou je všetko zakázať. Ak zamestnanec potrebuje AI pri práci, zákaz povedie iba k tomu, že bude používať vlastný účet – len teraz o tom nikto nebude vedieť ani toľko, koľko vedel predtým.

Oveľa lepšie funguje kombinácia technických opatrení a jasných pravidiel:

Opatrenie	Prínos
Definovať schválené AI nástroje	Zamestnanci vedia, čo môžu používať
Vytvoriť jednoduchú AI politiku	Zníženie rizika úniku dát
Monitorovať používané cloudové služby	Lepšia viditeľnosť Shadow IT
Zaviesť firemné cloudové úložisko	Menej osobných diskov
Pravidelne školiť zamestnancov	Prevencia ľudských chýb

Shadow IT nie je problém zamestnancov. Je to problém procesov.

Ak zamestnanci obchádzajú firemné nástroje, často tým hovoria:

„Potrebujeme jednoduchšie riešenie.“

Úlohou vedenia nie je hľadať vinníka. Úlohou je vytvoriť prostredie, kde sú bezpečné nástroje zároveň najjednoduchšie na používanie.

Prečo je táto téma dôležitá práve pre malé a stredné firmy?

Mnoho podnikateľov si myslí: „Máme 20 zamestnancov. Nás sa to netýka.“

Práve menšie firmy však často nemajú dedikované IT oddelenie ani nástroje na monitoring cloudových aplikácií. To znamená, že Shadow IT môže existovať celé mesiace bez povšimnutia.

Stačí niekoľko osobných Google Diskov, vlastných AI účtov alebo komunikácia cez WhatsApp a firma stráca prehľad nad tým, kde sa nachádzajú jej najcennejšie informácie.

Najčastejšie otázky

Je používanie ChatGPT vo firme nebezpečné? +

Nie. Rizikom nie je samotný nástroj, ale jeho používanie bez pravidiel. Firemné AI riešenia s podnikovými bezpečnostnými nastaveniami sú výrazne bezpečnejšie ako osobné účty.

Je WhatsApp vhodný na pracovnú komunikáciu? +

Na bežnú komunikáciu môže byť praktický, ale pri prenose citlivých firemných údajov často nespĺňa interné požiadavky na archiváciu, audit a správu dát.

Ako zistím, či máme vo firme Shadow IT? +

Najlepším začiatkom je audit používaných aplikácií, cloudových služieb a AI nástrojov, doplnený o rozhovory so zamestnancami.

Týka sa Shadow IT aj malých firiem? +

Áno. V menších firmách býva dokonca častejšie, pretože proces schvaľovania technológií býva neformálny a zamestnanci si nástroje vyberajú sami.

Záver

Shadow IT dnes nepredstavuje len niekoľko nepovolených aplikácií. Je to každodenná realita väčšiny firiem. Zamestnanci chcú pracovať efektívnejšie, no bez jasných pravidiel môžu nechtiac vytvárať bezpečnostné riziká.

V COMTEC pomáhame malým a stredným firmám získať prehľad nad používanými technológiami, nastaviť bezpečné využívanie AI nástrojov, chrániť firemné dáta a pripraviť IT prostredie na požiadavky dnešnej doby. Ak si nie ste istí, či sa Shadow IT týka aj vašej firmy, prvým krokom môže byť jednoduchý bezpečnostný audit a analýza používaných aplikácií.

Netušíte, koľko Shadow IT sa skrýva vo vašej firme?

Bezplatný audit kybernetickej bezpečnosti vám ukáže, kde sú vaše dáta a aké riziká hrozia – bez technického žargónu, zrozumiteľne.

Chcem bezplatný audit →

Alebo sa pozrite na naše služby:

Kybernetická bezpečnosť → Komplexná správa IT →

https://comtec.sk/novinky/shadow-it-najvacsie-bezpecnostne-riziko-o-ktorom-vacsina-majitelov-firiem-nevie