MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **31** ze dne **28.3.2023**

Zapomeňte na mýty o modelu nulové důvěry

Jedním z nejnovějších "módních trendů" v oblasti kybernetické bezpečnosti je model zabezpečení s nulovou důvěrou, označovaný jako "Zero Trust" (Zero Trust Network Access, ZTNA). Stručně řečeno, model nulové důvěry v podstatě znamená, že nenecháváte vůbec žádný prostor pro chyby a nevěříte nikomu a ničemu.

Díky hybridnímu pracovnímu prostředí, k němuž nás přivedly následky pandemie a různé, nově vznikající technologie, jako jsou Metaverse, Web 3.0 nebo rozšířená a virtuální realita, se odvětví kybernetické bezpečnosti jako obvykle usilovně snaží být co nejlépe připraveno na budoucnost. Protože ale na vývoj těchto technologií a jejich dopad teprve čekáme, musíme při jejich používání postupovat opatrně

Co je vlastně znamená nulová důvěra? Je to nový produkt? Jde o certifikaci? Nebo je to jen módní výraz z oblasti kybernetické bezpečnosti?

Některé organizace si mohou model nulové důvěry splést se skutečným produktem nebo certifikací. Ve skutečnosti však není ani kyberbezpečnostním produktem ani novou certifikací, ale přístupem, který se aplikuje za účelem zajištění komplexní kybernetické a cloudové bezpečnosti. Je nasazován pro zabezpečení interních i externích uživatelů, přičemž jedním z nejdůležitějších konceptů, kterými se řídí, je *"nikdy nedůvěřuj, vždy ověřuj"*. Přístup nulové důvěry mimo jiné zahrnuje i nasazení vícefaktorové autentizace za účelem udělení přístupu k jakékoli aplikaci nebo platformě, a mikrosegmentaci bezpečnostních perimetrů, aby se zabránilo rozšíření jakéhokoliv narušení bezpečnosti.

Žádné nové bezpečnostní prvky nebo přístupy nejsou zcela bez rizika, dokud nevybudujeme pravidla jejich používání a správné návyky mezi zaměstnanci. Stejně tak i přístup nulové důvěry je o budování dobrých návyků u zaměstnanců. Je zde důležité zajistit, aby zaměstnanci při přístupu k jakýmkoli aplikacím nebo platformám zapnuli vícefaktorové ověřování. Mluvíme zde o formě další vrstvy ověřování, kterou by neměl obcházet ani správce IT, někdo na nejvyšší úrovni nebo dokonce implementátor. Aby si organizace vybudovala lepší bezpečnostní pozici, je třeba zajistit přístup shora dolů a průběžně ověřovat a validovat všechny zaměstnance.

Model nulové důvěry ale není jen o vícefaktorovém ověřování. Vyžaduje, aby pro přístup k jakýmkoli aplikacím nebo datům byli průběžně ověřováni a autorizováni všichni uživatelé i jejich konfigurace zabezpečení. To se provádí další vrstvou zabezpečení, přičemž tento model má i různé výhody, jako možnost vzdálené autentizace a ověřování vašimi zaměstnanci, což jim umožní bezpečně pracovat na dálku nebo hybridním způsobem.

Lze přijmout model nulové důvěry kdykoli?

Před nasazením jakéhokoli nového modelu zabezpečení musíme znát návratnost investice. Musíme také vědět, zda jej skutečně potřebujeme. Je třeba pochopit, že model nulové důvěry je sice přístupem k zajištění zabezpečení nejdůležitějších aktiv podniku, ale stejně důležité je vědět, zda se nám nasazení tohoto modelu vyplatí.

Již ve chvíli, kdy se rozhodnete nasadit zabezpečení s nulovou důvěrou, musíte být digitální organizací, která má digitální aktiva, která potřebují cloudovou a kybernetickou ochranu. Současně by vaši zaměstnanci měli mít digitální zařízení, prostřednictvím kterých se mohou ověřit.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **31** ze dne **28.3.2023**

Nemusíme následovat každý módní trend a nasazovat každou novou technologii, která je právě uvedena na trh. Nejprve musíme pochopit své bezpečnostní potřeby a pak podle nich jednat. Investice do kybernetické bezpečnosti se vyplatí pouze tehdy, pokud se jí vy i vaši zaměstnanci budete ochotni dlouhodobě věnovat a vybudujete si správné návyky, abyste zajistili komplexní kyberbezpečnost.

Zdroj: SystemOnLine