Deloitte.

Mobilní bezpečnost
Mobile Security

Řízení podnikové mobility (EMM – Enterprise Mobility Management) je proces a systém, který umožňuje efektivně spravovat firemní a BYOD mobilní zařízení přistupující k datům společností. Organizace by měla být schopna tato zařízení a data spravovat, neboť mohou v případě jejich špatné správy představovat vysoké bezpečnostní riziko. EMM by tak mělo zajistit minimalizaci bezpečnostních rizik vynucením bezpečnostních zásad na jednotlivá zařízení a přístupná data.

Mobilita

Technologie současnosti přináší dnešním zaměstnancům dříve netušené možnosti. Mobilní zařízení různých typů dovolují zaměstnancům pracovat prakticky kdykoliv a kdekoliv, čímž zvyšují jejich efektivitu a tím také zisky společností, to má však také svou daň v podobě zvýšení bezpečnostních rizik plynoucích ze zapojení mobilních zařízení do systémů společnosti. Toto riziko je ještě vyšší, je-li zaměstnancům dovoleno přinášet si svá vlastní zařízení založená na různých technologiích.

Přínosy zavedení EMM

- Snížení nákladů na IT zařízení a nákladů Service Desku
- Zvýšení odolnosti organizace proti útokům ze spravovaných zařízení
- Zabezpečení vysoké mobility pracovníků
- Zvýšení spokojenosti a efektivity zaměstnanců

Mobilní (ne)bezpečnost

Bezpečnost operačního systému mobilních zařízení a v něm ukládaných citlivých dat je ohrožena uživateli, kteří na zařízení instalují různé aplikace. Nekontrolují nastavení práv a aplikace může zasílat citlivé informace vývojářům nebo distributorovi. Uživatelé svá zařízení „otevírají" kvůli využívání nepovolených funkcí, což významně snižuje úroveň bezpečnosti a umožňuje útoky. EMM a pravidla pro mobilní přístupy do interní sítě jsou základní podmínkou pro ochranu firemních dat.

Řízení podnikové mobility

Umožňuje, aby všechna používaná mobilní zařízení společnosti byla evidována, a jejich bezpečnost musí být prosazována v rámci všech úrovní organizace. Využitím systémů EMM je snadné ochránit veškerá data zpracovávaná na mobilních zařízeních, stejně jako přístupy do interních systémů společnosti. Systémy EMM dovolují vynutit bezpečnostní zásady, které tuto ochranu umožní.

Kompetence Deloitte

- Pracovníci s rozsáhlými zkušenostmi z oblastí výroby, financí a IT
- Kontinuální vzdělávání konzultantů pro EMM
- Znalosti z mezinárodních a velkých českých organizací
- Účast konzultantů na mnoha konferencích zaměřených na mobilní bezpečnost

S čím můžeme pomoci:

Řízení podnikové mobility

Bezpečnostní analýza stávajícího prostředí, definice funkčních a bezpečnostních požadavků pro zavedení efektivního a bezpečného systému správy mobilních zařízení pro podporu každodenních zaměstnaneckých úloh, návrh přístupů pro zavedení systému řízení podnikové mobility – zdroje, procesy a politiky pro efektivní řízení a zabezpečení mobilních zařízení a dat.

Výběr EMM řešení

Na základě výsledků analýzy prostředí a definice požadavků, výběr nejvhodnějšího řešení pro správu podnikové mobility (EMM).

Implementační studie wearables

Analýza podnikového prostředí a návrh případové studie implementace wearable zařízení pro podporu procesů a aktivity dané společnosti.

Návrh bezpečnosti mobilních aplikací

Analýza funkčních požadavků na navrhovanou mobilní aplikaci a návrh bezpečnostních požadavků pro zajištění bezpečného provozu dané aplikace a ochrany zpracovávaných dat.

Revize bezpečnosti a penetrační testování mobilních aplikací

Kontrola návrhu architektury a zabezpečení mobilní aplikace z hlediska bezpečného zpracování, ukládání a komunikace dat ve fázi jejího vývoje. Revize zdrojového kódu aplikace a implementovaných metod zpracování dat jak na straně mobilní aplikace, tak na straně aplikačního serveru.

Kontaktní informace: *Vlastimil Červený, Senior Manager*
+420 737 210 667, vcerveny@deloittece.com

Deloitte.

Mobile Security

Enterprise Mobility Management (EMM) is a process and system that enables efficient administration of corporate and BYOD mobile devices accessing company data. An organisation should be able to administer these devices and data, as they can represent a significant security threat if administered incorrectly. EMM should ensure the minimisation of security risks by enforcing security rules for the individual devices and accessed data.

Mobility

The technologies of today bring unprecedented possibilities to employees. Various types of mobile devices basically enable employees to work anytime and anywhere, which increases efficiency and company revenues, but the price is an increase in security risks arising from the connection of mobile devices to company systems. The risks are even higher if employees are allowed to bring in their own devices that use different technologies.

The benefits of introducing EMM

- Lower IT equipment and Service Desk costs
- Increased resilience of the organisation against attacks from the managed devices
- Ensuring the high mobility of employees
- Increased employee satisfaction and efficiency

Mobile (in)security

The security of the operating system of a mobile device and the sensitive data stored in it is jeopardised by users installing applications. Users don't verify the authorisation settings and as a consequence, it may happen that an application sends sensitive data to the developers or the distributor. Users "open" their devices in order to be able to use unauthorised functions, which significantly decreases the security level and opens the doors for attacks. EMM and rules on mobile access into the internal network are the basic prerequisite for the protection of company data.

Enterprise Mobility Management

EMM enables a company to keep records of all its mobile devices, while their security must be enforced on all levels of the given organisation. Using EMM systems, it is easy to protect all the data processed by mobile devices, and to control access into the company's internal systems. EMM systems make it possible to enforce security measures that enable the required protection.

Contact information

Vlastimil Červený, Senior Manager
+420 737 210 667, vcerveny@deloittece.com

Deloitte competence

- Employees with extensive experience in the manufacturing, finance and IT industries
- Continuous training of EMM advisors
- Knowledge gained in working with international and large Czech organisations
- Advisors' participation in many conferences on the topic of mobile security

What we can help with:

Enterprise Mobility Management
Security analysis of the existing environment, defining functional and security requirements on the implementation of an efficient and secure administration system of mobile devices supporting everyday employee tasks, proposed approach to the implementation of an EMM system – resources, processes and policies for the efficient management and protection of mobile devices and data.

Choosing the right EMM solution
Based on the environment analysis results and the definition of functional and security requirements, we will help you choose the most suitable EMM solution.

Wearables implementation study
Enterprise environment study and draft case study for the implementation of wearable devices supporting the processes and activities of the given company.

Mobile application security proposal
Analysis of the functional requirements for the proposed mobile application and a proposal of security requirements to ensure safe operation of the given application and protection of the processed data.

Security revision and penetration testing of mobile applications
Revision of the architecture design and of mobile application security in respect of safe data processing, saving and communication in the application's development phase. Revision of the application's source code and of the implemented data processing methods, both for the application and for the application server.