## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | * In the USB drive there is a lot of PII like family photos, family activities and even a CV. * Furthermore, there are sensitive work files like schedules and employee budgets. * It is unsafe to store personal files with work related ones. Not only that, but it is also highly unprofessional. |
| **Attacker mindset** | * The information could absolutely be used against employees; for example, the schedule could be used to break in or even kidnap an employee. * It could absolutely be used against relatives; for example, the photos could be used to identify them for nefarious purposes or even impersonate them. * It could absolutely be used to access the business since an attacker could exploit the leaked schedule to find a good time to break in and gain physical access to the business. |
| **Risk analysis** | * The company can make awareness campaigns against these types of incidents and the correct response to them. The company could also design periodic antivirus checks to find possible exploits, thus reducing risk of further damage. The computers could be set up with autoplay disabled so that even if the USB device is plugged, either code or executable programs wouldn’t be triggered automatically. |