Issue #1 E-mail unavailable.

**Short description:** e-mail is unavailable from Friday evening 28.10.2022  
**Type of issue:** logical  
**Impact:** retail, marketing, all other remote staff  
**Priority:** High  
**Full description:**Employees have not been able to access their e-mails or connect to Office 365 (or similar, e.g. Google Workplace) since Friday evening. IT support was informed about the disturbances at midday Saturday. An unauthorized person was detected connecting to the office’s local area computer network.

Working process

1. According IT operation agreement(SLA) – all Security incidents have the same priority.  
   Critical issues must be resolved on the day of occurrence. All responsible technical support engineers **must not** leave their workplaces until the e-mail service will be full recovery.  
   In case senior support engineers do not reach by phone they **must** come to the office immediately if they stay on the same city.
2. According SLA all employee who has detected first an issue **must** create request to the IT issue tracking system immediately on the day of occurrence.
3. The threat has wide impact, all employee affected. The business activity of the company is partially limited.
4. The company’s cyber security is under threat. Mail server under DDoS attack and doesn’t reach by network.
5. Threat refers to a logical threat. A server is virtual and can be replaced fast.
6. Only retail, marketing and other remote staff can’t doing their job because they use Office 365  
   mailbox day by day. Employee have noticed their leads about the problem. They have created workarounds and maximum save business activities in this case.
7. This issue has a high priority. In this case, the CEO may not be notified, only Deputy. Deputy check process of fixing and deadlines.
8. According the SLA, all affected leads and directors should be notified as soon as possible but not late then 1 hour