**Annex C**

(informative)

## Examples of typical threats

The following table gives examples of typical threats. The list can be used during the threat assessment process. Threats may be deliberate, accidental or environmental (natural) and may result, for example, in damage or loss of essential services. The following list indicates for each threat type where D (deliberate), A (accidental), E (environmental) is relevant. D is used for all deliberate actions aimed at information assets, A is used for all human actions that can accidentally damage information assets, and E is used for all incidents that are not based on human actions. The groups of threats are not in priority order.

|  |  |  |
| --- | --- | --- |
| **Type** | **Threats** | **Origin** |
| Physical damage | Fire | A, D, E |
| Water damage | A, D, E |
| Pollution | A, D, E |
| Major accident | A, D, E |
| Destruction of equipment or media | A, D, E |
| Dust, corrosion, freezing | A, D, E |
| Natural events | Climatic phenomenon | E |
| Seismic phenomenon | E |
| Volcanic phenomenon | E |
| Meteorological phenomenon | E |
| Flood | E |
| Loss of essential services | Failure of air-conditioning or water supply system | A, D |
| Loss of power supply | A, D, E |
| Failure of telecommunication equipment | A, D |
| Disturbance due to radiation | Electromagnetic radiation | A, D, E |
| Thermal radiation | A, D, E |
| Electromagnetic pulses | A, D, E |
| Compromise of information | Interception of compromising interference signals | D |
| Remote spying | D |
| Eavesdropping | D |
| Theft of media or documents | D |
| Theft of equipment | D |
| Retrieval of recycled or discarded media | D |
| Disclosure | A, D |
| Data from untrustworthy sources | A, D |
| Tampering with hardware | D |
| Tampering with software | A, D |
| Position detection | D |
| **Type** | **Threats** | **Origin** |
| Technical failures | Equipment failure | A |
| Equipment malfunction | A |
| Saturation of the information system | A, D |
| Software malfunction | A |
| Breach of information system maintainability | A, D |
| Unauthorised actions | Unauthorised use of equipment | D |
| Fraudulent copying of software | D |
| Use of counterfeit or copied software | A, D |
| Corruption of data | D |
| Illegal processing of data | D |
| Compromise of functions | Error in use | A |
| Abuse of rights | A, D |
| Forging of rights | D |
| Denial of actions | D |
| Breach of personnel availability | A, D, E |

Particular attention should be paid to human threat sources. These are specifically itemized in the following table:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Origin of threat** | | | **Motivation** | | | **Possible consequences** | | |
| Hacker, cracker | | | Challenge  Ego  Rebellion  Status  Money | | | * Hacking * Social engineering * System intrusion, break-ins * Unauthorized system access | | |
| Computer criminal | | | Destruction of information  Illegal information disclosure  Monetary gain  Unauthorized data alteration | | | * Computer crime (e.g. cyber stalking) * Fraudulent act (e.g. replay, impersonation, interception) * Information bribery * Spoofing * System intrusion | | |
| Terrorist | | | Blackmail  Destruction  Exploitation  Revenge  Political Gain  Media Coverage | | | * Bomb/Terrorism * Information warfare * System attack (e.g. distributed denial of service) * System penetration * System tampering | | |
| **Origin of threat** |  | | **Motivation** |  | | **Possible consequences** |
| Industrial espionage  (Intelligence, companies, foreign  governments, other government interests) | Competitive advantage  Economic espionage | | | * Defence advantage * Political advantage * Economic exploitation * Information theft * Intrusion on personal privacy * Social engineering * System penetration * Unauthorized system access (access   to classified, proprietary, and/or technology-related information) | | |
| Insiders  (poorly trained, disgruntled,  malicious, negligent, dishonest, or terminated employees) | Curiosity  Ego  Intelligence  Monetary gain  Revenge  Unintentional errors and omissions  (e.g. data entry error, programming error) | | | * Assault on an employee * Blackmail * Browsing of proprietary information * Computer abuse * Fraud and theft * Information bribery * Input of falsified, corrupted data * Interception * Malicious code (e.g. virus, logic bomb, Trojan horse) * Sale of personal information * System bugs * System intrusion * System sabotage * Unauthorized system access | | |