ANNEX A · INCIDENT CARDS

Print one copy per group of three and cut along the dashed lines. Every fact on these cards is real.

CASE 1 · WANNACRY · FRIDAY 12 MAY 2017

A program spreads by itself from one Windows computer to the next through the file-sharing port (445). It encrypts the files and asks for 300 dollars in bitcoin. In one day it reaches more than 200,000 computers in about 150 countries. Hospitals in England cancel about 19,000 appointments; Telefónica in Madrid tells its staff to switch off their PCs. Microsoft had published the update that closes the hole on 14 March 2017 — 59 days earlier.

CASE 2 · AJUNTAMENT DE CALVIÀ · SATURDAY 13 JANUARY 2024

In the early hours, criminals of the LockBit 3.0 group encrypt the town council's systems and ask for 10 million euros. The council refuses to pay, sets up a crisis committee, reports it to the Guardia Civil and rebuilds its systems; meanwhile many of its computer services are stopped. The later investigation found that the attackers got in through a vulnerability in one of the technologies the council used.

CASE 3 · EQUIFAX · 2017

Equifax keeps financial records of millions of people in the United States. On 7 March 2017 a fix is published for a flaw in a web framework the company uses (Apache Struts). An internal email asks the administrators to install it. One system is missed. Attackers enter through it and, unnoticed for weeks, copy the personal data of about 147 million people. The company announces it in September 2017.

CASE 4 · GITLAB.COM · 31 JANUARY 2017

Late at night, a tired engineer is repairing the copy of the main database. He types a command to delete a folder — in the terminal of the main server, not of the copy. He stops it after a second or two: about 300 GB are already gone. The team turns to the backups: none of the mechanisms they trusted works properly. They restore from a copy made by hand six hours earlier. Six hours of users' work are lost and the site is down for many hours. Nobody attacked anything.

CASE 5 · CROWDSTRIKE · FRIDAY 19 JULY 2024

CrowdStrike sells security software that companies install on their Windows computers. That morning it sends all of them an automatic update with an error in it. About 8.5 million computers show a blue screen and cannot start again; airports, banks, shops and hospitals around the world stop. Many of them have to be repaired by hand, one by one. It was not an attack.