Enkele kwetsbaarheden

DigiNotar (2011)

DigiNotar was een publicly trusted Certificate Authority (CA)en verzorgde de beveiliging van de elektronische communicatie door en tussen overheden (de zgn. Public Key Infrastructure of PKI). In 2011 werd dit bedrijf gehackt. Hierdoor kreeg een externe partij de mogelijkheid valse SSL-certificaten uit te geven en werden de certificaten onbruikbaar.

WannaCry (2017)

WannaCry (ook WannaCrypt, WanaCrypt0r 2.0 of Wanna Decryptor) is een ransomware ontwikkeld voor het Microsoft Windows besturingssysteem. WannaCry bestaat uit twee componenten: een ransomwarecomponent en een worm. Een uitbraak van dit ransomware heeft plaatsgevonden en het besmette daarbij meer dan 230.000 computers in 150 landen. Door de cyberaanval WannaCry viel een deel van de Britse gezondheidszorg uit.

NotPetya (2017)

NotPetya legde de productie van belangrijke medicijnen plat en kostte één van de grootste containerrederijen ter wereld honderden miljoen euro's.

Universiteit Maastricht (2019)

Cyberaanval waardoor de goede voortgang van het onderwijs en onderzoek tijdelijk in gevaar was. Tien dagen was de universiteit digitaal op slot waardoor medewerkers en studenten geen gebruik konden maken van het netwerk en de ICT-diensten van de universiteit.

Citrix (2020)

Ernstige kwetsbaarheid in 2 Citrix-servers: Citrix ADC en Citrix Gateway. Door deze kwetsbaarheid in het Citrix-systeem kunnen hackers toegang krijgen tot het computersysteem van uw organisatie.

Hof van Twente (2020)

Criminelen kwamen de systemen van de gemeente Hof van Twente binnen via een openstaande RDP-poort die kan worden gebruikt voor beheer op afstand. Door middel van een bruteforceaanval ofwel het proberen van grote hoeveelheden gebruikersnaam/wachtwoord-combinaties, kregen de aanvallers toegang tot een van de servers met een testbeheerdersaccount.

SolarWinds Orion (2021).

Volgens SolarWinds is de kwetsbaarheid opzettelijk gecreëerd door een actor, met als achterliggend doel om de systemen te compromitteren van de afnemers van de betreffende versie van SolarWinds Orion. Deze kwetsbaarheid

kan door kwaadwillenden worden misbruikt om toegang te krijgen tot bijvoorbeeld informatie of beheersfuncties van organisaties.

Log4J (2021)

Een Denial-of-Service-kwetsbaarheid van in Apache Log4j. Dit is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen. Het is een Log4Shell-gat in Java-tool Log4j. Ontwikkelaars gebruiken die logbestanden om te kijken of hun programma's naar behoren functioneren. Door de registraties te manipuleren kunnen hackers Log4J hun eigen, kwaadaardige code laten downloaden en uitvoeren.

Rode Kruis (2022)

Het Internationale Comité van het Rode Kruis (ICRC) in Genève (Zwitserland) werd slachtoffer van een geavanceerde cybersecurityaanval. Daarbij werden van zeker 515.000, vaak kwetsbare mensen de privégegevens weggenomen. De data is over de hele wereld gestolen, ook bij lokale verenigingen van het Rode Kruis.