Ordforklaring Cyberforsikring.

Hackerangreb
En ulovlig indtrængen i IT-systemet begået af en person, der ikke er ansat

Adgangskode

Med en stærk adgangskode menes en kode, som er bestående af mindst 8 tegn, der skiftes mindst hver 12. måned eller biometrisk godkendelse. Adgangskoden skal bestå af mindst en kombination af store og små bogstaver og tal. Adgangskoden må ikke indeholde navnet på sikrede, og må ikke være identisk med eller have stor lighed med brugernavn eller kodeord, som benyttes af andre hos sikrede.

Regelmæssigt (skift af adgangskode)
Med regelmæssigt menes, at adgangskoden ændres hver 12. måned. På den måde minimeres sandsynligheden for, at den kode som en kriminel måtte få fat i, faktisk fungerer. Jo oftere koden skiftes, desto mindre er sandsynligheden for, at den kode en hacker har fået fat i, er den nyeste.

Biometri
Biometri er brugen af biologiske målinger eller fysiske karakteristika, såsom fingeraftryk, ansigtsgenkendelse eller iris-scanning, til at identificere og verificere en persons identitet

Backup
En backup er en kopi af sikredes data, der gemmes et sikkert sted for at beskytte mod tab og skade. Hvis de originale data går tabt, kan de gendannes fra backuppen.

GF Forsikring anbefaler at anvende 3-2-1 backup-reglen af sikredes data. Herved kan data hurtigt kan genskabes og gendannes efter en dækningsberettiget skade. Reglen foreskriver at opbevare 3 kopier af sikredes data. På mindst 2 forskellige lagringsmedier. Hvor mindst 1 af kopierne er placeret et andet sted end sikredes netværk.

Virus
Ved virus forstås et program, der er udviklet til at sprede sig selv med den hensigt at påvirke eller skade indholdet i andre programmer, som ofte derved ødelægges. Et virusangreb er således forårsaget af en automatisk proces, der er blevet initieret fx ved, at en medarbejder hos sikrede har klikket på fx et link i en mail, klikket på et link på en hjemmeside mv

Cyberkrig
Cyberkrig, refererer til en bredere konflikt hvor der anvendes digitale angreb, der kan og ofte har til formål, at forårsage omfattende skade på it-infrastruktur og data hos sikrede. Angreb som disse kan resultere i betydelige økonomiske tab for sikrede.

Cyberkrigsførelse
Cyberkrigsførelse, refererer til brugen af digitale teknologier eller udstyr, til udførelse af angreb med det formål at forstyrre, sabotere, manipulere, destruere, eller gøre skade. Dette omfatter blandt andet hacking, malware, spredning af skadelig software som virus eller DDoS-angreb.

Cyberoperation
Cyberoperation, refererer til enhver handling udført af en stat eller dens agenter, med det formål at forstyrre, nægte adgang til, manipulere eller ødelægge informationssystemer, digitale strukturer, kritisk infrastruktur eller andre essentielle tjenester.

Terrorisme
Ved terrorisme forstås en handling, herunder men ikke begrænset til vold eller trussel om anvendelse af vold, foretaget af en person eller flere personer, uanset om de handler på egen hånd eller i forbindelse med en eller flere organisationer og/eller myndigheder, begået med politisk, religiøst, ideologisk eller etnisk formål eller begrundelse, herunder med den hensigt at påvirke en regering og/eller at sprede frygt i offentligheden eller dele af offentligheden.

For at karakterisere handlingen som terrorisme forudsættes, at handlingen er egnet til at påvirke en regering og/eller sprede frygt i offentligheden eller dele deraf.

NBCR-terrorskader
NBCR-terrorskader refererer til skader forårsaget af terrorangreb, der involverer nukleare, biologiske, kemiske eller radiologiske (NBCR) våben.

Hybridkrig
Hybridkrig, refererer til en kombination af angrebsmetoder der anvendes samtidig, eller forskudt af hinanden – og som er medvir kende til at skabe forvirring og udnytte sårbarheder.

Kryptovaluta
Kryptovaluta er en digital valuta, der bruger kryptografi til sikker hed og fungerer uden en central myndighed som bank. Eksempler inkluderer Bitcoin og Ethereum, som blandt andet bruges til beta linger, investeringer.

Data
Data og programmer, der kan indlæses i en computer, herunder softwaremæssig systemopsætning.

Phishing
Phishing refererer til cyberangreb, hvor angriberen forsøger at narre medarbejdere til at afsløre følsomme oplysninger som ad gangskoder, kreditkortnumre eller andre personlige data. Dette sker typisk gennem falske e-mails, beskeder eller websites, der ser ud til at komme fra en troværdig kilde.

Ransomware
Ransomware angreb udført med det formål at inficere sikredes PC'ere og krypterer brugernes filer og dokumenter. Herefter kræver hackerne løsepenge for at frigive filerne og dokumenterne igen.

Databehandler
Med en databehandler forstås en fysisk eller juridisk person, en virksomhed, offentlig myndighed, organisation n eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

Datterselskab
Som datterselskab anses juridiske personer (selskaber) i hvilke sikrede selv, eller sammen med andre sikrede, besidder mere end 50% af stemmerettighederne.

DDoS
DDoS står for Distributed Denial of Service, der har til formål at overbelaste og lamme et system. Forskellen er, at et DoS-angreb typisk udføres af én enhed, mens et DDoS-angre

MFA (Multifactor Authentication)
Multifaktorgodkendelse, i daglig tale MFA, er en sikker metode til at logge på netværk, systemer, programmer og servere med videre. MFA tilføjer et ekstra lag af sikkerhed ved at kræve, at brugeren bekræfter sin identitet med to eller flere faktorer.

OT-enheder
OT-enheder står for Operationel Teknologi-enheder. Disse enhe der omfatter hardware og software der bruges til at overvåge og styre processer og fysiske enheder.

Personoplysninger
Med personoplysninger forstås enhver form for information, der kan henføres til bestemte personer, eksempelvis personnummer, billede, registreringsnummer eller lignende

Social engineering
Social engineering er en metode, hvor svindlere manipulerer mennesker til at afsløre fortrolige oplysninger eller udføre handlinger, der kan kompromittere sikkerheden. Dette kan blandt andet ske via telefonopkald, SMS eller e-mail, hvor svindleren - i stedet for at bruge tekniske hacking metoder udnytter menneskers psykologi og tillid.

Tort
Særlig godtgørelse for krænkelse eller ydmygelse som tilføjes en person, så denne mister anseelse eller selvfølelse.