CYBER-GUIDEN

VAD DU BEHÖVER VETA OM CYBERVÄRLDEN

Irina Lönnqvist och Panu Moilanen

VARFÖR BEHÖVER DU DEN HÄR GUIDEN?

Cybervärlden kan tyckas vara något som bara experter behöver förstå sig på. Men det är inte sant, utan cybervärlden berör oss alla. Vi lever nämligen alla i cybervärlden varje dag.

Under de senaste årtiondena har vår vardag förändrats mycket snabbt, och det finns inga tecken på att takten skulle avta: tvärtom. I dag fungerar nästan hela vår vardag via datasystem, datanätverk och dataprogram – med andra ord i cybervärlden.

Lätt förenklat kan man säga att cybervärlden är en värld av bits, eller bitar. En bit är en informationsenhet i en form som kan förstås av datorer och kan ha värdet 1 eller 0. Allting i cybervärlden är uppbyggt av dessa bitar. Det kan jämföras med att allting i vår fysiska värld är uppbyggt av atomer.

Bitvärlden och atomvärlden går allt oftare in i varandra. Även om till exempel en tv-appa-

rat är ett fysiskt föremål, fungerar den inte utan bitar. På precis samma sätt behövs samspel mellan bitar och atomer till exempel inom handeln, hälso- och sjukvården eller trafiken. I samband med detta används ofta ordet digitalisering. Digitalisering innebär också att bitvärlden och cybervärlden blir en allt mer integrerad del av våra liv.

Cybervärlden och dess bitar påverkar med andra ord var och en av oss, och ingen kan längre välja att ställa sig utanför cybervärlden. Därför är det viktigt att vi alla känner till och förstår grunderna om cybervärlden. Därför lönar det sig också för dig att läsa den här guiden.

VAD HAR CYBERSÄKERHET MED VÅR VARDAG ATT GÖRA?

Vi har säkert alla åtminstone hört i nyheterna hur driftstörningar i olika datasystem har påverkat vanliga medborgares liv. Det har inte gått att betala med kort i närbutikens kassa, lönen har kanske inte kommit in på kontot i tid, eller också har det blivit kaos i stadstrafiken på grund av problem i systemet som styr trafiksignalerna.

DEN KRITISKA INFRASTRUKTUREN

Med kritisk infrastruktur avses alla de tjänster, system och strukturer som är livsviktiga för vårt samhälle. Som exempel på kritisk infrastruktur kan nämnas betalsystem, styrsystem för trafiken samt elnätet.

CYBERVÄRLDEN

Den kritiska infrastrukturen och cybervärlden är i dag så tätt sammanlänkade att de flesta system som hör till den kritiska infrastrukturen inte längre kan fungera om cybervärlden inte gör det. Oftast finns det inga alternativa sätt att utföra de uppgifter som systemen ska sköta. Därför är många vardagliga funktioner helt beroende av att cybervärlden fungerar.

SÄKERHET

Störningar i vardagen är tråkiga, och kan i värsta fall också orsaka betydande olägenheter och till och med fara. Framför allt är störningarna ändå en psykisk påfrestning: störningar i invanda funktioner och rutiner kan rubba vår trygghetskänsla och få oss att känna osäkerhet. Det här är normalt, och det är bra att redan i förväg fundera på hur vi ska reda oss om det skulle hända att de grundläggande funktionerna i vårt samhälle inte fungerar

som vanligt, till exempel på grund av problem i cybervärlden eller någon annan orsak.

ATT FÖRBEREDA SIG

När man funderar på sin egen strategi för att reda sig finns det mycket information som kan vara till hjälp. Allvarliga störningar i cybervärlden skulle påverka våra liv på i stort sett samma sätt som exempelvis ett omfattande strömavbrott. Därför lönar det sig att läsa Försvarsministeriets guide ”Strömmen gick”. Det är också bra att se till att ha ett reservförråd med mat och andra nödvändiga dagligvaror hemma för ungefär en veckas behov. Läs mer om reservförråd i broschyren Hemförråd, som getts ut av Räddningsbranschens Centralorganisation i Finland: WWW.SPEK.FI/PÅ-SVENSKA/BEREDSKAP/HEMFORRAD.

VAD BETYDER CYBER?

Cyber är inget ord i sig, utan används i sammansättningar. Alla termer som börjar på cyber syftar vanligen på behandling av information i elektronisk form, alltså informations- eller datateknik, dataöverföring och datasystem.

Cybervärlden påverkar den fysiska världen och den fysiska världen påverkar cybervärlden. De här världarna är förenade med varandra på många olika sätt. Dagens samhälle fungerar med hjälp av bitar. Cybervärlden kan till exempel ses som ett slags stad.

Men cyberstaden finns inte på kartan och har inga geografiska koordinater. Via nätet kan vi emellertid bland annat träffa folk och sköta våra dagliga ärenden i cyberstaden. Företagen är aktiva oavsett tid på dygnet. Cyberstaden sover aldrig.

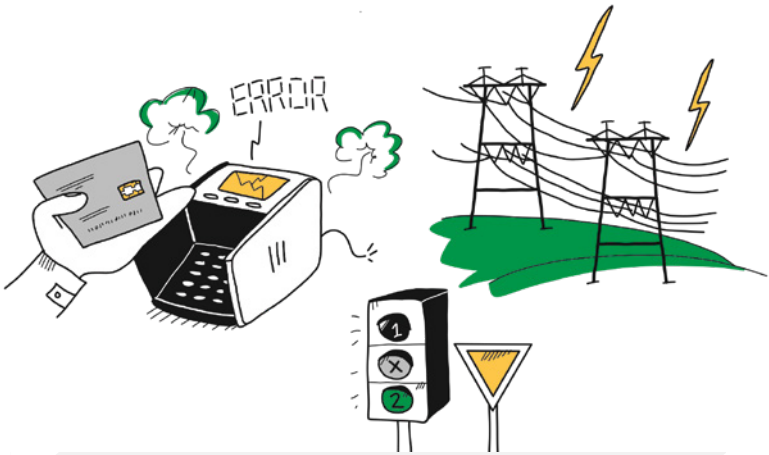
CYBERORDLISTA

Cyberrymden är en miljö som är avsedd för behandling av digital information och består av datorer och annan utrustning som kommunicerar med varandra samt av datanätverk.

Cybersäkerhet är säkerhet i cybervärlden. Det betyder att man har kontroll över de olika hot som riktas mot cybervärlden och att cybervärlden fungerar korrekt och felfritt. Då fungerar också den kritiska infrastruktur som är beroende av cybervärlden.

Cyberhot betyder risk för en handling eller en händelse som påverkar cybervärlden och som äventyrar cybervärldens korrekta och felfria funktion om hotet förverkligas.

Cyberförsvar är det delområde av cybersäkerheten som hänför sig till landets försvar. Cyberförsvar innefattar underrättelseverksamhet i och om cybervärlden, skydd av cybermiljöer som är viktiga med tanke på försvaret samt påverkan av vissa cybermiljöer. I Finland har Försvarsmakten ansvar för cyberförsvaret.



Informationspåverkan innebär att påverka innehållet i tillgänglig information och informationsgången samt därmed påverka slutresultatet för en händelsekedja i dess olika faser. Målet kan exempelvis vara att påverka medborgarnas åsikter.

IoT (Internet of Things), sakernas internet, betyder att internet utsträcks till apparater och maskiner som kan styras och mätas via nätet. Sakernas internet finns i allt fler människors vardag: till exempel kan tvättmaskinen vara ansluten till internet.

Kritisk infrastruktur är alla de tjänster, system och strukturer som är livsviktiga för vårt samhälle. Som exempel kan nämnas elnätet.

Överbelastningsattack är en nätattack i syfte att försöka förhindra att en viss onlinetjänst används på avsett sätt. Attacken genomförs oftast genom att rikta så mycket trafik mot tjänsten att den inte länge kan fungera normalt.

Phishing eller nätfiske är verksamhet i syfte att komma över konfidentiella uppgifter (till exempel person- eller kontouppgifter) genom att utge sig vara en aktör som har rätt att få dessa uppgifter. Med hjälp av dessa uppgifter kan man sedan försöka få exempelvis ekonomiska fördelar.

Uppdatering (programuppdatering) Programvaror är komplicerade och innehåller i praktiken alltid fel. Det kan också behövas nya egenskaper i programvarorna. Fel korrigeras och egenskaper läggs till genom att uppdatera programvarorna. Uppdatering innebär att programvaran ändras så att den tidigare versionen ersätts med en ny programversion.

Datasystem är ett system som består av människor, databehandlingsutrustning, dataöverföringsutrustning och programvaror och som har till syfte att genom databehandling effektivisera eller underlätta någon funktion eller göra en funktion möjlig.

Informationssäkerhet syftar på alla arrangemang i syfte att säkerställa informationens tillgänglighet, integritet och konfidentialitet. I informationssäkerhet ingår bland annat att säkerställa informationen, utrustningen, programvaran, dataförbindelserna och verksamheten. På individnivå innebär informationssäkerhet att skydda viktiga uppgifter och viktig utrustning.

Troll är ett meddelande eller en person vars primära syfte är att provocera, skapa konflikter eller få folk att skriva onödiga meddelanden. Troll brukar framföra en extrem åsikt om ett ämne genom att uttrycka sig nedlåtande om motståndarnas åsikt och utan att beakta andras argument.

Säkerhetskopiering är kopiering och lagring av viktig information på någon annan plats är den ursprungliga. Om den ursprungliga informationen försvinner eller förstörs, kan informationen återställas från säkerhetskopiorna.

HUR SER ETT BRA LÖSENORD UT?

Ett lösenord är bra om det är tillräckligt komplicerat så att man inte kan gissa sig till det eller få reda på det genom att pröva eller räkna sig fram. Men det är också väsentligt att man själv kommer ihåg lösenordet. Hur ska man då hitta på ett bra lösenord?

I stället för ett lösenord är det bättre att hitta på en lösenfras – för lösenord gäller att längre alltid är bättre, och när man själv har hittat på frasen kommer man också ihåg den. Ett extra skydd får du genom att exempelvis använda dialektala eller annars ovanligare ord och lägga till specialtecken och siffror.

Till exempel så här: Sidu4TipporKattnSomSkote!

I lösenordet kan du alltså använda bokstäver, siffror och specialtecken, men inte å, ä och ö. Det är bäst att använda olika lösenord för alla tjänster. Det finns också program för hantering av lösenord. I dem kan man samla alla sina lösenord.

VAD ÄR INFORMATIONSPÅVERKAN?

Det sägs att kunskap är makt. Därför pågår ständiga försök att påverka kunskapen – alltså informationen. Vardagliga exempel på påverkan av det här slaget är bl.a. reklam eller upplysningskampanjer, som försöker få oss att äta hälsosammare eller röra på oss mer.

Att påverka information är också ett viktigt element i mellanstatliga relationer och i kriser av olika slag. I sådana fall talar man om informationspåverkan eller informationskrigföring. Med detta avses att påverka medborgarna, beslutsfattarna och funktionsförmågan genom att styra den tillgängliga informationen och informationsgången.

TEKNIK

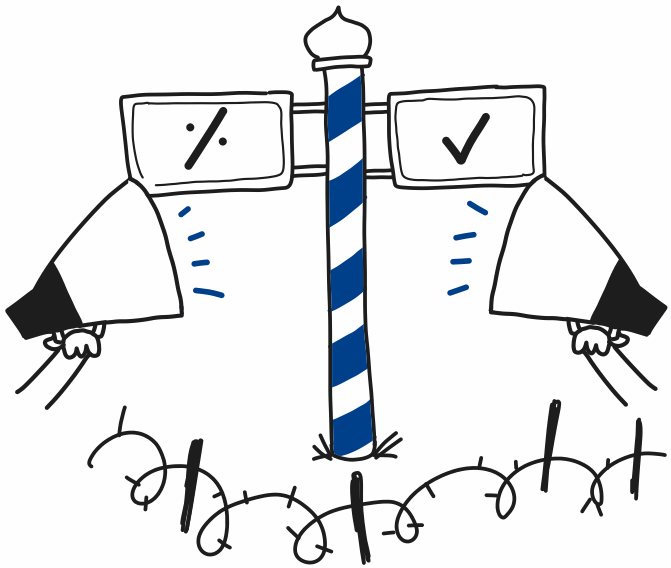
Tekniken har i hög grad förändrat kommunikationsmiljön också i Finland. Det är länge sedan de traditionella medierna hade monopol på kommunikationen, och i dag kan vem som helst nå ut till en mycket stor publik via internet och sociala medier. Därför går det i dag lättare – och ofta omärkbarare – än förut att bedriva informationspåverkan.

IFRÅGASÄTTANDE

Det är viktigt att vi inte utan att ifrågasätta tror på allt vi ser till exempel på sociala medier. Den information som förmedlas där kan vara avsiktligt förvriden eller helt felaktig. Det finns också hela webbplatser vars syfte är att sprida information som är felaktig eller som tjänar en viss aktörs intressen. Och då kan man tala om falska medier – emedan riktiga medier kontrollerar den information de förmedlar och strävar alltid till att ge möjligen felfri information, även om de många gånger har sina egna syften och mål.

KOMPETENS + KUNSKAP = SKYDD

För att skydda sig mot informationspåverkan behövs kompetens och kunskap. Det är alltid bra att försöka bedöma informationskällan utifrån den kunskap som finns om den, och det lönar sig att söka kunskap om samma ämnen från flera olika källor. Då kan man utveckla sin medieläskunnighet eller multiläskunnighet, som är en av de nya medborgarfärdigheterna i det moderna samhället.



HUR PÅVERKAR CYBERSÄKERHETEN JUST MIG?

När vi talar om cybersäkerhet kan vi också tala om informationssäkerhet. Alla digitala identiteter – exempelvis bankkoder och lösenord till olika tjänster – är information det lönar sig att skydda och vi vill skydda. Vi kan själva påverka detta exempelvis genom att hålla vår utrustning och programvaran uppdaterad och att använda antivirusprogram samt olika lösenord till olika tjänster.

Å andra sidan finns det också många saker vi inte kan påverka, men som det är viktigt att förstå. Många saker i vår vardag är kopplade samman i det uppkopplade samhället. Utan cybervärlden skulle det inte komma vatten från kranen eller el från eluttaget. Många funktioner är i hög grad beroende av att cybervärlden fungerar.

Med bondförnuft kommer man långt. Om något låter för bra för att vara sant, så är det ofta inte det. På sista sidan i guiden hittar du 'de tio plus ett cyberbudorden', som ger dig ger goda råd att förbättra både din egen och andras cybersäkerhet.

VILL DU VETA MER?

Blev du intresserad av cybersäkerhet, vill du veta och lära dig mer om det? Försvarsutbildningsföreningen MPK och Jyväskylä universitet har tillsammans gett ut den här guiden och ordnar vardera öppen utbildning för alla om cybersäkerhet. Läs mer om utbildningarna på WWW.MPK.FI och WWW.JYU.FI/IT/KYBER. Välkommen!

TEXT
Irina Lönnqvist (MPK)
Panu Moilanen (JYU)

ILLUSTRATIONER
Linda Saukko-Rauta
Redanredan Oy, 2017

LAYOUT
Ossi Hietala

UTGIVARE
Jyväskylä universitet och Försvarsutbildningföreningen MPK 2019

TRYCKERI
Jyväskylä/Raumo

ISBN
978-951-39-7975-1 (tryckt)
978-951-39-7976-8 (digital)

MÖJLIGGÖRARE
ICT-Suomi ry
Försörjnings-beredskapscentralen

MPK
MAANPUOLUSTUSKOULUTUSYHDISTYS
FÖRSVARSUTBILDNINGSFÖRENINGEN

JYU. Since 1863.

ICT SUOMI

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

MEDBORGARENS DE 10+1 CYBERBUDORDEN

1 Var alltid sunt misstänksam och, tillräckligt ofta, fråga varför.

2 Tänk alltid efter innan du lägger ut något på nätet: du behöver inte lägga ut allting och det som en gång lagts ut går inte längre att ta bort.

3 Kontrollera att den länk du tänker klicka på eller den bifogade fil du fått är äkta – vid minsta misstanke skall du kontakta exempelvis meddelandets avsändare.

4 Håll all din utrustning uppdaterad och sköt om informationssäkerheten. Om du inte själv vet hur man gör, be då en bekant eller en supporttjänst om hjälp. Informationssäkerheten är fel ställe att spara på. Var försiktig om du använder utrustning som inte är din egen.

5 Var särskilt noggrann när det handlar om pengar – till exempel kreditkorts- eller nätbanksuppgifter. Lämna aldrig ut dina personliga uppgifter om du inte är helt säker på till vem du lämnar dem.

6 Minns att offentliga och öppna trådlösa nätverk inte är säkra.

7 Minns att säkerhetskopiera.

8 Använd tillräckligt goda lösenord.

9 Om något låter för bra för att vara sant, så är det ofta inte det.

10 Cybervärldens fördelar är större än nackdelarna: var inte rädd i onödan!

+1 I mån av möjlighet, ta dig an också andras kompetens och informationssäkerhet – till exempel dina barn och föräldrar.