

eStudie.no – presenterer:

Datasikkerhet

- På jobben og privat

Skrevet av: Kjetil Sander © August 2020



Innholdsfortegnelse

INNHALDSFORTEGNELSE	2
1 DATASIKKERHET	6
1.1 HVA ER DATASIKKERHET?	6
1.2 HVORFOR ER DATASIKKERHET VIKTIG?	6
1.3 HVOR GODT HAR DU SIKRET DITT NETTVERK, OG DIN DATAMASKIN, NETTBRETT OG MOBIL?	6
1.4 IKKE GLEM DIN FACEBOOK KONTO OG DITT NETTBRETT OG SMARTTELEFON SOM ER BLITT HACKERNES NYE FAVORITTER	7
1.5 SIKKERHETSSJEKK FOR BEDRIFTER	7
2 SIKKERHETSTRUSLER	8
2.1 DATAVIRUS	8
2.1.1 Hva er et datavirus og hvorfor heter det virus?	8
2.1.2 Hvordan spres datavirusene?	8
2.1.3 Hvorfor er virus farlige?	9
2.1.4 Hvilke virustyper finnes?	9
2.1.5 Hva er et virusbibliotek?	10
2.1.6 Hva er hoax-virus?	10
2.1.7 Hva er muterende virus?	11
2.1.8 Hva er en Patch?	11
2.2 MALWARE	11
2.2.1 Hva er malware?	11
2.2.2 Keylogger	11
2.2.3 Skremselsprogram (Scareware)	12
2.2.4 Adware	12
2.2.5 Rootkits	12
2.3 ORM	13
2.4 TROJANER (TROJANSK HEST)	14
2.4.1 Hvordan smitter trojanske hester min maskin?	14
2.4.2 Hvem angriper trojanske hester?	14
2.4.3 Hvilken skade kan en trojansk hest gjøre?	15
2.5 DDOS ANGREP	16
2.5.1 Definisjon	16
2.5.2 Slik ser et DDoS angrep ut	17
2.5.3 Metoder for angrep	17
2.5.4 Typer DDoS Angrep	18
2.5.5 Hvordan kan du beskytte deg mot DDoS angrep?	19
2.5.6 Brannmurer	19
2.5.7 Switches	20
2.5.8 Rutere	20
2.5.9 Applikasjonsserver for bredbåndstyring foran server parken	20
2.5.10 IPS forebygging	20
2.5.11 DDS baserte forsvar	21
2.5.12 Blackholing og sinkholing	21
2.5.13 Rene rør	21
2.6 BAKDØR	22
2.7 BOTNET, OGSÅ KALT ZOMBIES	22
2.7.1 Hva er en bot?	22
2.7.2 Hvordan en bot fungerer?	23
2.7.3 Hvilken skade kan et botnet gjøre?	24
2.7.4 Hvordan brukes et botnet til kriminelle handlinger?	24

2.7.5	Types of attacks	25
2.8	BRUTE FORCE	25
3	DE VANLIGSTE SIKKERHETSHULLENE.....	27
3.1	DÅRLIG PASSORD.....	27
3.2	IKKE OPPDATERT UTSTYR OG PROGRAMVARE.....	27
3.3	MANGLENDE VIRUSPROGRAM.....	27
3.4	MANGLENDE BRANNMUR	27
3.5	ÅPEN LINJE/KOMMUNIKASJON	27
3.6	MANGLENDE SUNN FORNUFT.....	28
3.7	PASSORDREGLER	28
3.7.1	<i>Dette er passordene hackere prøver seg med.....</i>	28
3.7.2	<i>Hvordan velge gode passord?.....</i>	30
3.7.3	<i>Benytt minst åtte bokstaver i ditt passord.....</i>	30
3.7.4	<i>Benytt både små og store bokstaver.....</i>	31
3.7.5	<i>Lag en enkel huskeregel.....</i>	31
3.7.6	<i>Bytt ut bokstaver med tall.....</i>	31
3.7.7	<i>Ikke bruk ord som finnes i en ordbok eller på et språk.....</i>	31
3.7.8	<i>Ikke bruk passord basert på personlig informasjon</i>	32
3.7.9	<i>Velg en vanlig ord + årstall + første stavelse av tjenesten</i>	32
3.7.10	<i>Lag naturlige spesialtegn</i>	32
3.7.11	<i>Ikke bruk det samme passordet overalt</i>	33
3.7.12	<i>Bytt passord ved jevne mellomrom</i>	33
3.7.13	<i>Husk at folk er forutsigbare – det samme er du.....</i>	33
3.7.14	<i>Ikke benytt «husk passord funksjonen» som ofte tilbys.....</i>	34
3.7.15	<i>Pass godt på ditt passord</i>	34
3.7.16	<i>Ingenting er helt sikkert</i>	34
3.8	SURFE-REGLER PÅ INTERNETT	35
3.8.1	<i>Dette er (som regel) ikke farlig.....</i>	35
3.8.2	<i>Dette KAN være risikabelt</i>	35
3.8.3	<i>Dette ER risikabelt.....</i>	35
3.8.4	<i>Grunnregler.....</i>	36
3.9	E-POSTREGLER FOR SIKKER EPOST	37
3.9.1	<i>Bruk hue.....</i>	37
3.10	SLIK BESKYTTER DU DEG MOT SPAM.....	38
3.10.1	<i>Bruk flere e-postadresser !</i>	38
3.10.2	<i>Hver kreativ i valg av e-postadresse.....</i>	38
3.10.3	<i>Bytt e-post adresse jevnlig</i>	38
3.10.4	<i>Skru av auto-svar, feriemeldinger og sykemeldinger</i>	39
3.10.5	<i>Ikke legg din e-post adresse på egne nettsider i klartekst.....</i>	39
3.10.6	<i>Skru av HTML-visning</i>	39
3.10.7	<i>Skru av bilde- og forhåndsvisning.....</i>	40
3.10.8	<i>Bruk alltid en oppdatert versjon av din nettleser og e-postprogram</i>	40
3.10.9	<i>Sørg for at du har et skikkelig spamfilter på både server og klientnivå</i>	40
3.10.10	<i>Sjekk hvilke RBL-filtre ditt spamfilter er satt opp mot.....</i>	41
3.10.11	<i>Opprett en SPF-record i sone-filen til ditt domenenavn</i>	41
3.10.12	<i>Hver forsiktig med å angi e-postadressen din på Internett.....</i>	41
3.10.13	<i>Ikke åpn mistenkelig e-post eller e-post fra ukjente avsendere</i>	42
3.10.14	<i>Svar aldri på spam!.....</i>	42
3.10.15	<i>Klikk aldri på en URL eller nettadresse i en spam melding</i>	42
3.10.16	<i>Vær kritisk til «unsubscribe» funksjonen i spam fra ukjent.....</i>	43
3.10.17	<i>Prøv aldri et anti-spam nettsted.....</i>	43
4	BRANNMUR.....	44
4.1	FUNKSJON	44

4.2 PERSONLIG BRANNMUR	45
4.3 TRUSLER	45
4.4 TYPER AV BRANNMURER	45
4.5 VIRKEMÅTE	45
4.5.1 Applikasjonsfokusert	45
4.5.2 Trafikkfokusert	45
4.6 INSTALLASJON	46
4.7 BRUK	46
4.7.1 Applikasjonsfokuserte	46
4.7.2 Trafikkfokuserte	47
4.8 LOGGER	47
4.9 MER BISTAND	47
5 SIKRING AV TRÅDLØSE NETTVERK (WI-FI)	48
5.1 WEP – DEN STORE SYNDEREN	48
5.2 WPA – KRYPTERINGEN ER IKKE STERKERE ENN PASSORDET	48
5.3 WPS – DEN SKJULTE SÅRBARHETEN	49
5.4 Å SKJULE NETTVERKET ER INGEN GOD LØSNING	50
5.5 LOGG INN PÅ RUTERENS ADMINISTRASJONGRENSESNIITT	50
5.6 OPPDATER FIRMWARE (OPERATIVSYSTEMET)	50
5.7 BYTT TIL ET UNIKT NETTVERKNAVN	51
5.8 IKKE SKJUL NETTVERKNAVN	51
5.9 IKKE BRUK WEP ELLER WPS	51
5.10 BRUK WPA2 MED AES-KRYPTERING	51
5.11 BRUK ET GODT PASSORD PÅ DET TRÅDLØSE NETTVERKET	51
5.12 ..OG PÅ RUTERENS KONFIGURASJONSIDE	52
5.13 SLÅ AV FJERNADMINISTRASJON	52
5.14 MAC-FILTRERING ER IKKE TILSTREKKELIG	52
5.15 TRENGER DU UPNP?	52
5.16 EN BEDRE DNS?	53
5.17 SJEKK TILKOBLEDE ENHETER	53
6 SIKRING AV DATAMASKINER	54
6.1 HVER FORSIKTIG MED WINDOWS OG ANDROID	54
6.2 SKAFF DEG EN PERSONLIG BRANNMUR	54
6.3 SKAFF DEG ET ANTI-VIRUS PROGRAM	54
6.4 STENG ALLE ÅPNE PORTER PÅ DATAMASKINEN	54
6.5 HOLD MASKINEN OG PROGRAMMENE OPPDATERT	54
6.6 PASSORDBESKYTT SENSITIVE FILER OG MAPPER	55
7 SIKRING AV MOBILTELEFON OG NETTBRETT	56
7.1 MOBILTELEFONER OG NETTBRETT MÅ HÅNTERES PÅ SAMME MÅTE SOM DATAMASKINER	56
8 SSL SECURE SOCKETS LAYER	58
8.1 TRYGG OVERFØRING AV DATA OG TRANSAKSJONER!	58
8.2 SIKKERHETEN AVGJØRES AV KRYPTERINGSLGORITMEN	58
8.3 HVORFOR SSL?	58
8.4 BRUKSOMRÅDER FOR SSL	59
8.5 KRYPTERING OVER TCP/IP – NIVÅET	60
8.6 HVA ER TCL (TRANSPORT LAYER SECURITY)?	61
8.7 KRYPTERTE PORTER	61
8.8 NETTLESERGJENKJENNELSE	61
8.9 TRANSAKSJONSFORSIKRING	62
8.10 UTSTEDES AV ET SERTIFISERINGORGAN	62
8.11 HVORDAN SER JEG AT EN NETTSIDE BRUKER SSL?	62

8.12 ANBEFALING.....	62
9 SIKKERHETSKOPIERING.....	63
9.1 HVA KAN SKJE MED LAGRET INFORMASJON	63
9.2 HVILKE INFORMASJON SKAL SIKRES.....	63
9.3 GODE VANER ER VIKTIG.....	63
9.4 TYPER SIKKERHETSKOPI	63
9.5 INTERN OPPBEVARING	64
9.6 EKSTERN OPPBEVARING	64
9.7 TYPER AV LAGRINGSMEDIA	64
9.7.1 CD og DVD.....	64
9.7.2 Minnepinner.....	64
9.7.3 Ekstern harddisk.....	64
9.7.4 Datatape/ kassett	65
9.7.5 Online tjenester.....	65
10 HVA MÅ DU HUSKE PÅ NÅR DU KASTER DIN PC, MAC, KAMERA ELLER MOBIL?	66
10.1 HUSK Å SLETT ALL SENSITIV INFORMASJON	66
10.2 DET HOLDER IKKE Å BARE TRYKKE PÅ «DELETE»	66
10.3 SJEKKLISTE:	66
10.3.1 PC	67
10.3.2 Mobiltelefon.....	67
10.3.3 Digitalkamera.....	67
10.4 ANSVAR FOR SIKKER SLETING	67
11 HVEM STÅR JURIDISK ANSVARLIG FOR SIKRINGEN OG INNHOLDET I NETTSKYEN?	68
11.1 VIRKSOMHETEN ER JURIDISK ANSVARLIG.....	68
11.2 HVILKET ANSVAR HAR NETTSKY LEVERANDØREN?	68
11.3 RISIKOVURDERING OG INFORMASJONSSIKKERHET	69
11.4 INFORMASJONSPLIKT.....	69
11.5 SÆRLIGE PROBLEMSTILLINGER.....	70
11.6 DET GJELDER Å HOLDE TUNGA RETT I MUNNEN	70
11.7 SJEKKLISTE	71
11.8 NOEN BANALE SIKKERHETSREGLER	71