enisa

DEN EUROPÆISKE UNIONS AGENTUR
FOR CYBERSIKKERHED

Vejledning om cybersikkerhed til SMV'er

12 TRIN TIL AT SIKRE DIN VIRKSOMHED

Covid-19-krisen viste tydeligt, hvor stor betydning internettet og computere generelt har for SMV'er. For at kunne drive deres forretning videre under pandemien var mange SMV'er nødt til at træffe kontinuitetstiltag, blandt andet begynde at anvende cloud computingtjenester, forbedre deres internettjenester, opgradere deres websteder og give personalet mulighed for at arbejde hjemmefra.

Denne brochure indeholder 12 overordnede trin, som SMV'er kan tage for at sikre deres systemer og virksomhed. Brochuren er et supplement til den mere detaljerede ENISA-rapport **"Cybersecurity for SMES – Challenges and Recommendations"**.

1 SKAB EN GOD CYBERSIKKERHEDSKULTUR

UDDELEGER LEDELSESANSVAR

God cybersikkerhed er afgørende for SMV'ers fortsatte succes. Ansvaret for denne kritiske funktion bør tildeles en person i virksomheden, som kan sikre, at der afsættes tilstrækkelige ressourcer til cybersikkerhed i form af mandtimer, at der indkøbes software, tjenester og hardware i forbindelse med cybersikkerhed, at personalet får uddannelse i emnet, og at der udarbejdes effektive strategier for cybersikkerhed.

VIND OPBAKNING FRA DE ANSATTE

Vind medarbejdernes opbakning gennem effektiv kommunikation fra ledelsen om cybersikkerhed, ledelsens åbne støtte til initiativer vedrørende cybersikkerhed, specifik uddannelse til medarbejderne og klare og specifikke regler for medarbejderne samlet i cybersikkerhedspolitikker.

OFFENTLIGGØR CYBERSIKKERHEDSPOLITIKKER

Virksomheden skal have cybersikkerhedspolitikker med klare og specifikke regler for den adfærd, de ansatte forventes at udvise, når de anvender virksomhedens IKT-udstyr, -tjenester og -faciliteter. Disse politikker skal også tydeliggøre konsekvenserne, hvis en medarbejder ikke overholder reglerne. Politikkerne skal revideres og opdateres regelmæssigt.

GENNEMFØR CYBERSIKKERHEDSREVISIONER

Der bør gennemføres regelmæssige revisioner af personer med den fornødne viden, de nødvendige færdigheder og den fornødne erfaring. Revisorerne skal være uafhængige, og det kan enten være en ekstern entreprenør eller en intern revisor fra virksomheden, som ikke have noget med den daglige IT-drift at gøre.

HUSK DATABESKYTTELSE

I henhold til EU's databeskyttelsesforordning[1] skal alle SMV'er, der behandler eller lagrer personoplysninger om borgere fra EU-/EØS, sikre den fornødne sikkerhedskontrol for at beskytte sådanne oplysninger. Dette indebærer også, at sikre, at eventuelle tredjeparter, der arbejder for virksomheden, har de fornødne sikkerhedsforanstaltninger på plads.

1 Generel forordning om databeskyttelse https://ec.europa.eu/info/law/-topic/data-protection_da

2

TILBYD RELEVANTE KURSER

Tilbud regelmæssige kurser i cyberbevidsthed til alle medarbejdere for at sikre, at de kan genkende og håndtere de forskellige cybertrusler. Disse kurser bør skræddersyes til SMV'en og fokusere på konkrete eksempler fra hverdagen.

Tilbyd specialiserede kurser i cybersikkerhed til dem, der er ansvarlige for håndteringen af cybersikkerhed i virksomheden, for at sikre, at de har de fornødne færdigheder og kompetencer, der kræves til jobbet.

3

SØRG FOR EFFEKTIV HÅNDTERING AF TREDJEPARTER

Sørg for, at alle leverandører, navnlig dem, der har adgang til følsomme oplysninger og/eller systemer, håndteres aktivt og overholder de aftalte sikkerhedskrav. Der skal foreligge aftaler om, hvordan leverandørerne skal opfylde disse sikkerhedskrav.

4

UDARBEJD EN BEREDSKABSPLAN

Udarbejd en formel beredskabsplan, som indeholder klare retningslinjer, roller og ansvarsområder, som sikrer, at alle sikkerhedshændelser håndteres på en rettidig, professionel og passende måde. For hurtigt at kunne reagere over for trusler kan du undersøge, hvilke værktøjer der kan overvåge og sende varslinger, når der opstår mistænkelige aktivitet, eller der sker overtrædelser af sikkerheden.

5 SØRG FOR SIKKER SYSTEMADGANG

Tilskynd alle til at anvende en passphrase, en gruppe af mindst tre vilkårlige og almindelige ord, der kombineres til en sætning, som både er let at huske og sikker. Hvis du vælger et almindeligt password:

- Sørg for, at det er langt, består af små og store bogstaver, eventuelt også tal og specialtegn.
- Undgå oplagte valg af passwords, f.eks. "password" eller bogstav - og talrække som "abc" eller "123".
- Undgå at anvende personlige oplysninger, som kan findes på nettet.

Uanset om du anvender passphrases eller passwords

- Anvend dem ikke andre steder.
- Del dem ikke med kollegaer.
- Aktivér multifaktorautentificering.
- Anvend en særlig password-manager.

6 SIKRE ENHEDER

En central del af cybersikkerhedsprogrammet er at sørge for, at de enheder, medarbejderne anvender, er sikre, uanset om det er desktopcomputer, bærbare computere, tabletcomputere eller smartphones.

SØRG FOR AT INSTALLERE PATCHES OG OPDATERINGER AF SOFTWARE

Anvend helst en central platform til patch-håndtering. SMV'er bør:

- regelmæssigt opdatere deres software
- aktivere automatiske opdateringer, når det er muligt
- identificere software og hardware, der kræver manuel opdatering
- tage højde for mobile enheder og IoT-enheder.

VIRUSBESKYTTELSE

En centralt styret virusbeskyttelsesløsning bør installeres på alle enheder og holdes opdateret for at sikre, at den fortsat er effektiv. Pas på ikke at installere piratprogrammer, da de kan indeholde skadeligt software.

ANVEND VÆRKTØJER, DER BESKYTTER E-MAILS OG WEB

Anvend løsninger, der blokerer spammails og e-mails med links til skadelige websteder og skadelige vedhæftninger, som kan indeholde virus, samt phishingmails.

KRYPTERING

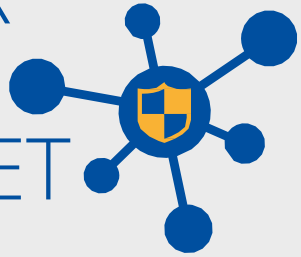
Beskyt data gennem kryptering. SMV'er bør sikre, at data lagret på mobile enheder, f.eks. bærbare computere, smartphones og tabletcomputere, er krypterede. Sørg for, at data, der overføres via offentlige netværk, f.eks. wi-fi-netværk på hoteller eller i lufthavne, krypteres, enten gennem et VPN (virtuelt privatnet) eller ved at anvende en sikker forbindelse via en SSL-/TLS-protokol for adgang til websteder. Sørg for, at egne websteder anvender egnet krypteringsteknologi for at beskytte kundedata, som overføres via nettet.

ANVEND HÅNDTERING AF MOBILENHEDER

For at lette hjemmearbejde tillader mange SMV'er medarbejdere at anvende deres egne bærbare computere, tabletcomputere og/eller smartphones. Det medføre alvorlige sikkerhedsproblemer med hensyn til de følsomme forretningsdata, der er lagret på de enheder. En måde at håndtere denne risiko på er at anvende en MDM-løsning (Mobile Device Management), hvilket giver virksomheden mulighed for at:

- kontrollere, hvilke enheder der får adgang til deres systemer og tjenester
- sikre, at enheden har et opdateret virusprogram installeret
- kontrollere, at enheden er krypteret
- bekræfte, at enheden har opdaterede patches installeret
- sørge for, at enheden er beskyttet af en PIN-kode og eller et password
- fjerne alle virksomhedens data fra enheden, hvis enhedens indehaver anmelder, at den er forsvundet eller blevet stjålet, eller hvis indehaverens ansættelse i virksomheden ophører.

7 SØRG FOR AT SIKRE NETVÆRKET



ANVEND FIREWALLS

Firewalls styrer al trafik ud og ind af netværket, og er et kritisk værktøj til at beskytte virksomhedens systemer. Firewalls bør anvendes til at beskytte alle kritiske systemer, og navnlig til at beskytte virksomhedens netværk fra internettet.

GENNEMGÅ FJERNADGANGSLØSNINGER

SMV'er bør regelmæssigt gennemgå alle fjernadgangsværktøjer for at garantere, at de er sikre. De bør navnlig:

- sørge for, at alle patches og opdateringer i software, der anvendes til fjernadgang, fungerer
- begrænse fjernadgang fra mistænkelig geografiske lokaliteter eller visse IP-adresser.
- begrænse medarbejdernes fjernadgang til kun at omfatte de systemer og computere, de har brug for til deres arbejde.
- kræve stærke passwords til fjernadgang og om muligt aktivere multifaktorautentificering
- sikre at overvågnings- og varslingsfunktioner, som advarer om formodede angreb eller usædvanlig mistænkelig aktivitet, er aktiveret.

8 GØR DEN FYSISKE SIKKERHED BEDRE

Der bør anvendes passende fysisk kontrol der, hvor der lagres vigtig information. En virksomheds bærbare computer eller smartphone bør f.eks. ikke ligge uden opsyn på bagsædet af en bil. Hver gang en bruger forlader sin computer, bør den låses. Alternativt kan der også aktiveres en automatisk låsefunktion på alle enheder, der anvendes til arbejdsbrug. Følsomme trykte dokumenter må heller ikke efterlades uden opsyn, og når de ikke bruges, skal de låses inde.

9 SIKRE BACKUPS

For at kunne genskabe vigtig information er det vigtigt at have backupfiler, da det er en effektiv måde at genoprette data efter katastrofer, såsom ransomwareangreb.
Følgende regler bør anvendes vedrørende backup:

- Backup skal ske regelmæssigt og automatisk, når det er muligt
- Backupfiler skal holdes adskilt fra virksomhedens produktionsmiljø
- Backupfiler skal krypteres, navnlig hvis de flyttes mellem forskellige lokaliteter
- Muligheden for regelmæssigt at gendanne data fra backup skal afprøves Der skal helst gennemføres en regelmæssig afprøvning af fuld gendannelse af data fra start til slut.

10

CLOUDTJENESTER

Der er mange fordele ved cloudbaserede løsninger, men de er også forbundet med en del unikke risici, som SMV'er bør overveje, inden de vælger en cloududbyder. ENISA har offentliggjort "Cloud Security Guide for SMEs"[2], som SMV'er bør læse, inden de migrerer til cloud.

Når SMV'er vælger en cloududbyder, bør de sikre sig, at de ikke overtræder nogen love eller bestemmelser ved at lagre data, navnlig persondata, uden for EU/EØS. EU's persondataforordning kræver f.eks., at personoplysninger om indbyggere i EU/EØS ikke lagres eller overføres uden for EU/EØS, undtagen under helt særlige omstændigheder.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 SØRG FOR AT SIKRE ONLINE WEBSTEDER

SMV'er skal sørge for, at deres online websteder er konfigureret og vedligeholdt på en sikker måde, og at alle persondata eller bankoplysninger, såsom oplysninger om kreditkort, er beskyttet på behørig vis. Dette indebærer regelmæssige sikkerhedstjek af websteder for at identificere eventuelle svagheder med hensyn til sikkerheden og regelmæssige revisioner for at sikre korrekt opdatering og vedligeholdelse af websteder.

12 SØG OG DEL INFORMATION

Et effektivt værktøj i kampen mod cyberkriminalitet er deling af information. Deling af information i forhold til cyberkriminalitet er vigtig for SMV'er for bedre at kunne forstå, hvilke risici de står over for. Det er mere sandsynligt, at virksomheder, der hører om udfordringer med cyberkriminalitet fra deres konkurrenter, og hvordan de håndterede dem, vedtager foranstaltninger, end hvis de får lignende information fra erhvervsrapporter eller cybersikkerhedsundersøgelser.

DEN EUROPÆISKE UNIONS AGENTUR FOR CYBERSIKKERHED

OM ENISA

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA har til formål at bidrage til målsætningen om et højt fælles niveau af cybersikkerhed i Europa. Den Europæiske Unions Agentur for Cybersikkerhed blev oprettet i 2004 og videre styrket ved EU's forordning om cybersikkerhed. Det bidrager til EU's politik for cybersikkerhed, fremmer troværdigheden af IKT-produkter, -tjenester og -processer gennem ordninger for cybersikkerhedscertificering, samarbejder med medlemsstater og EU-organer og ruster Europa til morgendagens cybersikkerhedsudfordringer. Gennem videndeling, kapacitetsopbygning og oplysningskampagner samarbejder agenturet med sine centrale interessenter om at styrke tilliden til den netforbundne økonomi, om at øge EU-infrastrukturens modstandskraft og om i sidste instans at garantere EU's og EU-borgernes digitale sikkerhed. Yderligere oplysninger findes på www.enisa.europa.eu.

ENISA

Den Europæiske Unions Agentur for Cybersikkerhed

Kontoret i Athen

Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki,
Grækenland

Kontoret i Heraklion

95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Grækenland

enisa.europa.eu