AĠENZIJA TAL-UNJONI EWROPEA GĦAĊ-ĊIBERSIGURTÀ

Gwida dwar iċ-ċibersigurtà għall-SMEs

12 -IL PASS

BIEX TIŻGURA N-NEGOZJU TIEGĦEK

Il-kriżi tal-COVID-19 uriet kemm huma importanti l-Internet u l-kompjuters b'mod ġenerali għall-SMEs. Sabiex jirnexxu fin-negozju matul il-pandemija, ħafna SMEs kellhom jieħdu miżuri ta' kontinwità tan-negozju, bħall-adozzjoni ta' servizzi tal-cloud, it-titjib tas-servizzi tal-internet tagħhom, l-aġġornament tas-siti web tagħhom u l-għoti ta' opportunità lill-persunal biex jaħdem mill-bogħod.

Dan il-fuljett jipprovdi lill-SMEs bi 12-il pass prattiku ta' livell għoli dwar kif jistgħu jiżguraw aħjar is-sistemi tagħhom u n-negozju tagħhom. Din hija pubblikazzjoni ta' akkumpanjament għar-rapport aktar dettaljat tal-ENISA **"Iċ-Ċibersigurtà għall-SMES – Sfidi u Rakkomandazzjonijiet".**

1 ŻVILUPPA KULTURA TAĊ-ĊIBERSIGURTÀ TAJBA

ASSENJA R-RESPONSABBILTÀ MANIĠERJALI

Iċ-ċibersigurtà tajba hija element ewlieni fis-suċċess kontinwu ta' kwalunkwe SME. Jenħtieġ li r-responsabbiltà għal din il-funzjoni kritika tiġi assenjata lil xi ħadd fl-organizzazzjoni li jenħtieġ li jiżgura li riżorsi xierqa bħal żmien mill-persunal, ix-xiri ta' software, servizzi u hardware taċ-ċibersigurtà, it-taħriġ għall-persunal, u l-iżvilupp ta' politiki effettivi, jingħataw liċ-ċibersigurtà.

IKSEB IL-PARTEĊIPAZZJONI TAL-IMPJEGATI

Ikseb il-parteċipazzjoni tal-impjegati permezz ta' komunikazzjoni effettiva dwar iċ-ċibersigurtà mill-maniġment, billi l-maniġment jappoġġa b'mod miftuħ l-inizjattivi taċ-ċibersigurtà, billi jingħata taħriġ xieraq lill-impjegati, u billi l-impjegati jiġu pprovduti b'regoli ċari u speċifiċi deskritti fil-politiki taċ-ċibersigurtà.

IPPUBBLIKA L-POLITIKI TAĊ-ĊIBERSIGURTÀ

Jenħtieġ li jiġu deskritti regoli ċari u speċifiċi fil-politiki taċ-ċibersigurtà għall-impjegati dwar kif huma mistennija jġibu ruħhom meta jużaw l-ambjent, it-tagħmir u s-servizzi tal-ICT tal-kumpanija. Dawn il-politiki jenħtieġ li jenfasizzaw ukoll il-konsegwenzi li jista' jiffaċċja impjegat jekk ma jikkonformax mal-politiki. Il-politiki jeħtieġ li jiġu riveduti u aġġornati regolarment.

WETTAQ AWDITI TAĊ-ĊIBERSIGURTÀ

Jenħtieġ li jitwettqu awditi regolari minn dawk bl-għarfien, bil-ħiliet u bl-esperjenza xierqa. L-awdituri jenħtieġ li jkunu indipendenti, kemm jekk ikunu kuntrattur estern kif ukoll kuntrattur intern għall-SMEs u indipendenti mill-operazzjonijiet tal-IT ta' kuljum.

FTAKAR FIL-PROTEZZJONI TAD-*DATA*

Skont ir-Regolament Ġenerali tal-UE dwar il-Protezzjoni tad-*Data*[1], kwalunkwe SME li tipproċessa jew li taħżen *data* personali li tappartjeni għar-residenti tal-UE/taż-ŻEE jeħtieġ li tiżgura li jkun hemm kontrolli tas-sigurtà xierqa fis-seħħ biex tiġi protetta dik id-*data*. Dan jinkludi l-iżgurar li kwalunkwe parti terza li taħdem f'isem l-SMEs ikollha fis-seħħ miżuri ta' sigurtà xierqa.

1 Ir-Regolament Ġenerali dwar il-Protezzjoni tad-*Data* https://ec.europa.eu/info/law/law-topic/data-protection_mt

2

IPPROVDI TAĦRIĠ XIERAQ

Ipprovdi taħriġ regolari ta' sensibilizzazzjoni dwar iċ-ċibersigurtà għall-impjegati kollha biex tiżgura li dawn ikunu jistgħu jirrikonoxxu u jittrattaw id-diversi theddidiet taċ-ċibersigurtà. Dan it-taħriġ għandu jitfassal għall-SMEs u għandu jiffoka fuq sitwazzjonijiet ta' ħajja reali.

Ipprovdi taħriġ speċjalizzat fiċ-ċibersigurtà għal dawk responsabbli għall-ġestjoni taċ-ċibersigurtà fi ħdan in-negozju biex tiżgura li jkollhom il-ħiliet u l-kompetenzi meħtieġa biex jagħmlu xogħolhom.

3

ŻGURA ĠESTJONI EFFETTIVA TA' PARTIJIET TERZI

Żgura li l-bejjiegħa kollha, b'mod partikolari dawk b'aċċess għal *data* u/jew għal sistemi sensittivi, ikunu ġestiti b'mod attiv u jissodisfaw il-livelli miftiehma ta' sigurtà. Jenħtieġ li jkun hemm fis-seħħ ftehimiet kuntrattwali li jirregolaw kif il-bejjiegħa jissodisfaw dawk ir-rekwiżiti ta' sigurtà.

4

ŻVILUPPA PJAN TA' RISPONS GĦALL-INĊIDENTI

Żviluppa pjan formali ta' rispons għall-inċidenti, li jkun fih linji gwida, rwoli u responsabbiltajiet ċari dokumentati biex jiġi żgurat li l-inċidenti kollha ta' sigurtà jiġu indirizzati b'mod f'waqtu, professjonali u xieraq. Biex tirrispondi malajr għat-theddid għas-sigurtà, investiga għodod li jistgħu jimmonitorjaw u joħolqu allerti meta jseħħu attivitajiet suspettużi jew ksur tas-sigurtà.

5 ASSIGURA L-AĊĊESS GĦAS-SISTEMI

Ħeġġeġ lil kulħadd juża passphrase, ġabra ta' mill-inqas tliet kelmiet komuni każwali kkombinati flimkien fi fraži li tipprovdi taħlita tajba ħafna ta' memorabilità u sigurtà. Jekk tagħżel password tipika:

- Agħmilha twila, b'karattri tal-ittri żgħar u kbar, possibbilment ukoll numri u karattri speċjali.
- Evita li tkun ovvja, bħal "password", sekwenzi ta' ittri jew numri bħal "abc", numri bħal "123".
- Evita l-użu ta' informazzjoni personali li tista' tinstab online.

U kemm jekk tuża passphrases jew passwords

- Terġax tużahom xi mkien ieħor.
- Tgħidhomx lill-kollegi.
- Ippermetti l-awtentikazzjoni b'diversi fatturi.
- Uża maniġer iddedikat tal-passwords.

6

APPARATI SIKURI

Iż-żamma tal-apparat li juża l-persunal, kemm jekk ikunu l-kompjuters desktop, il-laptops, it-tablets, jew l-ismartphones tagħhom, hija pass ewlieni fi programm taċ-ċibersigurtà.

ŻOMM IS-SOFTWARE KORRETT U AĠĠORNAT

Idealment bl-użu ta' pjattaforma ċentralizzata għall-ġestjoni tas-software korrettiv. Huwa rrakkomandat ħafna li l-SMEs:

- Jaġġornaw regolarment is-software kollu tagħhom.
- Jaqilbu fuq aġġornamenti awtomatiċi kull meta jkun possibbli.
- Jidentifikaw software u hardware li jeħtieġu aġġornamenti manwali.
- Iqisu l-apparat mobbli u tal-IoT.

ANTI-VIRUS

Jenħtieġ li tiġi implimentata soluzzjoni antivirus ġestita ċentralment fuq it-tipi kollha ta' apparati u li din tinżamm aġġornata sabiex tiġi żgurata l-effettività kontinwa tagħha. Barra minn hekk, tinstallax software kkupjat peress li jista' jkun fih malware.

UŻA GĦODOD TAL-PROTEZZJONI TAL-POSTA ELETTRONIKA U TAL-WEB

Uża soluzzjonijiet biex timblokka l-posta elettronika spam, posta elettronika li fiha links għal siti web malizzjużi, posta elettronika li jkun fiha hemżiet malizzjużi bħal viruses, u posta elettronika ta' phishing.

KRIPTAĠĠ

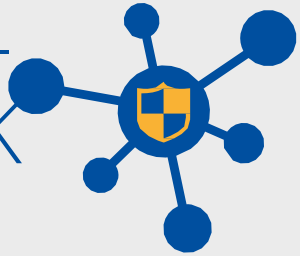
Ipproteġi d-*data* billi tikkriptaha. L-SMEs jenħtieġ li jiżguraw li d-*data* maħżuna fuq apparati mobbli bħal laptops, smartphones, u tabelli tkun kriptata. Għad-*data* ttrasferita fuq networks pubbliċi, bħal networks tal-WiFi tal-lukandi jew tal-ajruporti, jiġi żgurat li d-*data* tkun kriptata, jew billi jintuża Network Privat Virtwali (VPN) jew billi jiġu aċċessati siti web fuq konnessjonijiet siguri bl-użu tal-protokoll tal-SSL/TLS. Jiżguraw li s-siti web tagħhom stess ikunu qed jużaw teknoloġija ta' kriptaġġ xierqa biex jipproteġu d-*data* tal-klijenti hekk kif tivvjaġġa fuq l-Internet.

IMPLIMENTA L-ĠESTJONI TAL-APPARAT MOBBLI

Meta l-persunal jiġi ffaċilitat biex jaħdem mill-bogħod, ħafna SMEs jippermettu lill-persunal juża l-laptops, it-tablet u/jew l-ismartphones tiegħu stess. Dan jintroduċi diversi tħassib dwar is-sigurtà dwar id-*data* sensittiva tan-negozju maħżuna fuq dawk l-apparati. Mod wieħed kif jiġi mmaniġġjat dan ir-riskju huwa li tintuża soluzzjoni għall-ġestjoni tal-apparat mobbli (MDM), li tippermetti lill-SMEs:

- Jikkontrollaw liema apparati huma permessi jaċċessaw is-sistemi u s-servizzi tiegħu.
- Jiżguraw li l-apparat ikollu installat software aġġornat kontra l-virus.
- Jiddeterminaw jekk l-apparat huwiex kriptat.
- Jikkonfermaw jekk l-apparat għandux software korrettiv aġġornat installat.
- Jinfurzaw li l-apparat ikun protett b'PIN u/jew b'password.
- Ineħħu mill-bogħod kwalunkwe *data* dwar l-SME mill-apparat f'każ li s-sid tal-apparat jirrapportah mitluf jew misruq, jew jekk l-impjieg tas-sid tal-apparat mal-SME kellu jintemm.

7 ŻGURA N-NETWORK TIEGĦEK



UŻA FIREWALLS

Il-firewalls jimmaniġġaw it-traffiku li jidħol u li joħroġ minn network u huma għodda kritika fil-protezzjoni tas-sistemi tal-SMEs. Il-firewalls għandhom jintużaw biex jipproteġu s-sistemi kritiċi kollha, b'mod partikolari firewall għandu jintuża biex jipproteġi n-network tal-SMEs mill-Internet.

AGĦMEL RIEŻAMI TA' SOLUZZJONIJIET TA' AĊĊESS MILL-BOGĦOD

L-SMEs għandhom jirrevedu regolarment kwalunkwe għodda ta' aċċess mill-bogħod biex jiżguraw li dawn ikunu siguri, b'mod partikolari:

- Jiġi żgurat li s-software kollu ta' aċċess mill-bogħod huwa patched u aġġornat.
- Jirrestringu l-aċċess mill-bogħod minn postijiet ġeografiċi suspettużi jew minn ċerti indirizzi tal-PI.
- Jirrestringu l-aċċess mill-bogħod tal-persunal biss għas-sistemi u għall-kompjuters li jeħtieġu għax-xogħol tagħhom.
- Jinfurzaw passwords b'saħħithom għal aċċess mill-bogħod u fejn possibbli jippermettu awtentikazzjoni b'diversi fatturi.
- Jiżguraw li l-monitoraġġ u l-allertar ikunu attivati biex iwissu dwar attakki suspettati jew attività suspettuża mhux tas-soltu.

8 TEJJEB IS-SIGURTÀ FIŻIKA

Għandhom jintużaw kontrolli fiżiċi xierqa kull fejn ikun hemm residenti informazzjoni importanti. Pereżempju, laptop ta' kumpanija jew smartphone, ma għandhomx jitħallew weħidhom fis-sit ta' wara ta' karozza. F'kull ħin li utent imur lil hinn mill-kompjuter tiegħu għandu jsakkru. Inkella, jippermetti l-funzjoni tal-awtolock fuq kwalunkwe apparat użat għal skopijiet ta' negozju. Id-dokumenti sensittivi stampati ma għandhomx jitħallew waħedhom u meta ma jkunux qed jintużaw, għandhom jinħażnu b'mod sikur.

9 ARA LI L-BACKUPS IKUNU SIKURI

Sabiex ikun jista' jsir l-irkupru ta' informazzjoni ewlenija, għandu jsir backup peress li huwa mod effettiv biex isir irkupru minn diżastri bħal attakk ta' ransomware. Jenħtieġ li japplikaw ir-regoli ta' backup li ġejjin:

- il-backup għandu jkun regolari u awtomatizzat kull meta jkun possibbli,
- il-backup għandu jinżamm separatament mill-ambjent tal-produzzjoni tal-SMEs,
- il-backup għandu jkun kriptat, speċjalment jekk ikun se jiġi mċaqlaq minn post għall-ieħor,
- tiġi ttestjata l-kapaċità li tiġi rrestawrata b'mod regolari d-*data* mill-backup. Idealment, għandu jsir test regolari ta' restawr sħiħ mill-bidu sal-aħħar.

10

INVOLVI RUĦEK MAL-CLOUD

Filwaqt li joffru ħafna vantaġġi, is-soluzzjonijiet ibbażati fuq il-cloud jippreżentaw xi riskji uniċi, li l-SMEs għandhom jikkunsidraw qabel ma jinvolvu lil fornitur tal-cloud. L-ENISA ppubblikat "Gwida dwar is-Sigurtà tal-Cloud għall-SMEs"[2] li l-SMEs għandhom jirreferu għaliha meta jemigraw lejn il-cloud.

Meta jagħżlu fornitur tal-cloud, l-SMEs jenħtieġ li jiżguraw li ma tkun qed tinkiser l-ebda liġi jew regolament meta jaħżnu d-*data*, speċjalment id-*data* personali, barra mill-UE/iż-ŻEE. Pereżempju, il-GDPR tal-UE jeħtieġ li d-*data* personali tar-residenti fi ħdan l-UE/iż-ŻEE ma tinħażinx jew ma tiġix trażmessa barra mill-UE/iż-ŻEE sakemm dan ma jsirx taħt kundizzjonijiet speċifiċi ħafna.

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

11 ŻGURA S-SITI ONLINE

Huwa essenzjali li l-SMEs jiżguraw li s-siti web online tagħhom ikunu kkonfigurati u miżmuma b'mod sigur u li kwalunkwe *data* personali jew dettalji finanzjarji, bħad-*data* dwar il-karti ta' kreditu, ikunu protetti kif xieraq. Dan jinvolvi t-twettiq ta' testijiet regolari tas-sigurtà kontra s-siti web biex tiġi identifikata kwalunkwe dgħufija potenzjali fis-sigurtà u t-twettiq ta' rieżamijiet regolari biex jiġi żgurat li s-sit jinżamm u jiġi aġġornat kif xieraq.

12 FITTEX U KKONDIVIDI L-INFORMAZZJONI

Għodda effettiva fil-ġlieda kontra ċ-ċiberkriminalità hija l-kondiviżjoni tal-informazzjoni. Il-kondiviżjoni tal-informazzjoni fir-rigward taċ-ċiberkriminalità hija kruċjali għall-SMEs biex jifhmu aħjar ir-riskji li jiffaċċjaw. Id-ditti li jisimgħu dwar l-isfidi taċ-ċibersigurtà, u kif dawk l-isfidi ġew megħluba, mill-pari tagħhom x'aktarx jieħdu passi biex jiżguraw is-sistemi tagħhom milli kieku kellhom jisimgħu dettalji simili mir-rapporti tal-industrija jew mill-istħarriġiet taċ-ċibersigurtà.

AĠENZIJA TAL-UNJONI EWROPEA GĦAĊ-ĊIBERSIGURTÀ

DWAR ENISA

L-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà, ENISA, hija l-aġenzija tal-Unjoni ddedikata biex jinkiseb livell komuni għoli ta' ċibersigurtà fl-Ewropa kollha. Stabbilita fl-2004 msaħħa mill-Att tal-UE dwar iċ-Ċibersigurtà, l-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà tikkontribwixxi għall-politika ċibernetika tal-UE, issaħħaħ l-affidabbiltà tal-prodotti, is-servizzi u l-proċessi tal-ICT bi skemi ta' ċertifikazzjoni taċ-ċibersigurtà, tikkoopera mal-Istati Membri u l-korpi tal-UE u tgħin lill-Ewropa tħejji għall-isfidi ċibernetiċi tal-futur. Permezz tal-kondiviżjoni tal-għarfien, il-bini tal-kapaċità u s-sensibilizzazzjoni, l-Aġenzija taħdem flimkien mal-partijiet ikkonċernati ewlenin tagħha biex issaħħaħ il-fiduċja fl-ekonomija konnessa, biex iżżid ir-reżiljenza tal-infrastruttura tal-Unjoni, u, fl-aħħar mill-aħħar, biex iżżomm is-soċjetà u ċ-ċittadini tal-Ewropa siguri b'sens diġitali. Għal aktar informazzjoni, żur www.enisa.europa.eu.

ENISA

Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà

Uffiċċju ta' Ateni

Ethnikis Antistaseos 72 u
Agamemnonos 14,
Chalandri 15231, Attiki, il-Greċja

Uffiċċju ta' Heraklion

95, Nikou Plastira
700 13 Vassilika Vouton,
Heraklion, il-Greċja

enisa.europa.eu