Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Negozji żgħar gwida dwar is-sigurtà diġitali

Kumplessità tal-kontenut
SEMPLIĊI ● ○ ○

cyber.gov.au

Introduzzjoni

Għall negozju żgħir, anke inċident ċkejken tas-sigurtà diġitali jista' jkollu impatti qerrieda. Din il-gwida tinkludi miżuri bażiċi tas-sigurtà biex jgħinuk tipproteġi n-negozju tiegħek kontra theddid komuni tas-sigurtà diġitali. Biex nibdew, nirrakkommandaw dawn it-tlett miżuri li ġejjin:

- Attiva l-awtentikazzjoni multi-fattorali
- Aġġorna s-software tiegħek
- Agħmel back-up tal-informazzjoni tiegħek

Din il-gwida tista' tinkludi miżuri li mhumiex rilevanti għan-negozju tiegħek, jew in-negozju tiegħek jista' jkollu iktar bżonnijiet kumplessi. Wara li tispiċċa din il-gwida, nirrakkommandaw li negozji żgħar jimplimentaw L-Ewwel Livell ta' Maturità mit- Tmienja Essenzjali. Jekk għandek xi mistoqsijiet dwar dan il-parir jew dwar is-sigurtà diġitali iktar inġenerali, nirrakkommandaw li titkellem ma' professjonista tal- IT jew konsulent li tafda.

Żur cyber.gov.au biex taqra l-gwida sħiħa tagħna, inkluż parir dwar x'għandek tagħmel ('how-to') għal kull miżura.

Werrej tal-kontenut

Theddid għal negozji żgħar

Messaġġi qarrieqa

Scams huma mezz komuni li jużaw persuni kriminali biex jattakkaw negozji żgħar diġitalment. L-għan tagħhom huwa li jqarrqu bik jew bl-istaff tiegħek biex:

- jibgħatu flus jew gift cards
- jiklikkjaw fuq links jew affarijiet mehmużin malizzjużi
- Joffru informazzjoni sensittiva, bħal passwords.

Il-kriminali tas-cyber jistgħu jippruvaw u jqarrqu bin-negozju tiegħek permezz tal-imejl, messaġġi b'text, telefonati u l-midja soċjali. Huma sikwit jippretendu li huma persuna jew organizzazzjoni li inti tafda.

Attakki ta' Phishing

Ta' nkwiet partikolari għan-negozji żgħar huma l-attakki **msejħa phishing.** Dawn l-iscams sikwit ikollhom fihom link għal websajt falza fejn tkun inkoraġġut biex tilloggja f'kont jew iddaħħal dettalji kunfidenzjali.

Attakki ta' phishing tipikament ipoġġuf'kompromess/periklu il-passwords tal-kont tiegħek. Il-kriminali sikwit jużaw dan il-metodu biex iwettqu 'takeover' ta' kontijiet tal-midja soċjali ta' negozji żgħar u jitolbuhom prezz għall-fidwa.

Modi ta' mitigazzjoni

Jekk messaġġ ikun ġej minn entità magħrufa u jkun jidher suspettuż, uża kawtela. Ikkuntattja lill-persuna jew lin-negozju separatament biex tiċċekkja jekk il-messaġġ huwiex validu. Uża dettalji tal-kuntatt li ssib minn sors validu, bħal per eżempju billi żżur il-websajt uffiċjali tan-negozju, u mhux dawk fil-messaġġ suspettuż.

Iktar informazzjoni dwar kif tidentifika scams u attakki ta' phishing permezz tar-riżorsi li ġejjin:

- Agħraf u rrapporta scams
- Tgħallem kif tinnota scams ta' phishing
- Kif tinduna b'messaġġi maħduma soċjalment (Socially Engineered Messges)

Studju ta' każ:

Impjegata ta' kumpanija tal-kurjer irċeviet imejl minn wieħed/waħda mill-istaff eżekuttiv tagħha, fejn talab/talbet li hija tixtri 6 karti tal-kreditu MasterCard mħallsa minn quddiem, ta' $500 il-waħda. L-istaff eżekuttiv qalilha biex iżżomm dan f'kunfidenza għaliex il-karti se jkunu gift vouchers għall-membri tal-istaff. Ladarba xtrathom, l-impjegata ġiet mitluba tieħu ritratt taż-żewġ naħiet tal-karti tal-kreditu u tibgħathom lill-istaff eżekuttiv bħala provi tax-xiri tagħhom.

Skont l-istruzzjonijiet, l-impjegata marret f'uffiċju tal-posta u wżat il-karta tal-kreditu personali tagħha biex tixtri l-gift cards. Hija wieġbet l-imejl tal-istaff eżekuttiv u bagħtet ir-ritratti tal-gift cards bħala provi.

Wara li rritornat lura mill-uffiċju tal-posta, l-impjegata tat il-gift cards lill-istaff eżekuttiv - li ma kellux/kellhiex ideja tagħhom. Wara investigazzjoni, **instab li l-imejls kollha dwar il-gift cards kienu ġew minn indirizz addoċċ u ma kienux mill-kont veru tal-imejls tal-istaff eżekuttiv. Kien kollu scam.**

Attakki b'imejl

Barra scams bħal phishing, attakk komuni b'imejl kontra negozji żgħar huwa **business email compromise** (BEC) (kompromess b'imejl ta' negozju). Persuni kriminali jistgħu jippretendu li huma rappreżentanti tan-negozju billi jużaw kontijiet tal-imejl kompromettenti/suspettużi, jew permezz ta' mezzi oħra - bħall-użu ta' isem prinċipali li jidher simili għal dak ta' negozju ta' veru. Barra mis-serq tal-informazzjoni, l-għan ta' dawn l-attakki normalment huwa biex iqarraq bil-vittmi biex dawn jibgħatu fondi f'kont bankarju li jkun operat mill-persuna kriminali.

Modi ta' mitigazzjoni

L-aħjar difiża kontra attakki b'imejl huwa taħriġ u għarfien għall-impjegati tiegħek. Aċċerta li l-istaff tiegħek jafu biex ikunu dejjem attenti dwar imejls li jkollhom dan li ġej:

- talbiet ta' ħlas, speċjalment jekk ikunu urġenti jew li suppost ġa tħallsu
- tibdil ta' dettali bankarji
- indirizz tal-imejl li pjuttost ma jidhirx korrett, bħal fejn l-isem prinċipali tal-kumpanija ma jaqbilx eżattament mal-isem veru tal-kumpanija.

Filwaqt li dawn l-attakki jistgħu jkunu ta' ħsara kbira, il-miżuri ta' mitigazzjoni huma faċli u ma jiswew kważi xejn. **Meta l-istaff jirċievi imejls bħal dawn, l-iktar mod effettiv biex tnaqqas ħsara huwa li ssejjaħ lil min ikun bagħat l-imejl biex tikkonferma li huwa/hija validu/a.** Tużax id-dettalji tal-kuntatti li jkunu ntbagħtulek għax dawn jistgħu jkunu qarrieqa. Introduċi proċess formali biex isegwih l-istaff meta jirċievi talbiet għall-ħlas jew meta id-dettalji bankarji jiġu mibdula.

Tgħallem kif tipproteġi n-negozju tiegħek minn scams permezz ta' BEC, u kompromessi b'imejl, b'dawn ir-riżorsi li ġejjin:

- Kompromess b'imejl ta' negozju
- Ipproteġi n-negozju tiegħek minn qerq u kompromess b'imejl
- X'għandek tagħmel jekk in-negozju tiegħek huwa l-mira ta' frodi jew kompromess b'imejl.

Studju ta' każ:

Negozju żgħir tal-kostruzzjoni rċieva imejl mingħand il-fornitur tiegħu fejn qallu li biddel il-bank tiegħu. Il-fornitur ipprovda d-dettalji tal-kont il-ġdid biex isiru l-ħlasijiet. Billi l-imejl deher validu, **in-negozju tal-kostruzzjoni ma ċempilx lill-fornitur biex jikkonferma l-bidla fid-dettalji tal-kont bankarju.**

In-negozju ħallas fattura li rċeva mingħand il-fornitur ta' iktar minn $70,000. L-għada, impjegat ieħor bi żball reġa ħallas l-istess fattura għall-ammont addizzjonali ta' iktar minn $70,000. B'kollox, iktar minn $150,000 tħallsu fil-kont bankarju l-ġdid.

Meta n-negozju ċempel lill-fornitur tiegħu biex jitolbu jrodd lura l-ħlas doppju li kien sar, il-fornitur avża li dawk id-dettalji bankarji kienu inkorretti. Investigazzjoni bdiet immedjatament, u l-fornitur skopra li wieħed mill-kontijiet tal-imejls tiegħu kien ġie mbagħbas u kien qiegħed jibgħat dettalji ta' kontijiet bankarji qarrieqa. **L-ebda fondi ma ġew irkuprati.**

Software malizzjuż

Malware huwa terminu ġenerali għall-software malizzjuż iddisinjat biex jikkawża ħsara, bħal ransomware, viruses, spyware u trojans. Malware jista':

- Jisraq jew isakkar files fuq it-tagħmir diġitali tiegħek
- Jisraq in-numri tal-bank jew karta tal-kreditu tiegħek
- Jisraq il-usernames u passwords tiegħek
- Jieħu l-kontroll ta' jew jispjuna fuq il-kompjuter tiegħek.

Malware jista' jwaqqaf it-tagħmir diġitali tiegħek milli jaħdem tajjeb, ineħħi jew jikkorrompi files tiegħek, jew iħalli oħrajn jiksbu aċċess għall-informazzjoni tiegħek personali jew tan-negozju. Jekk it-tagħmir tiegħek huwa nfettat bil-malware, tista' tkun vulnerabbli għal attakki oħra. Il-malware jista' anke jinfirex għal tagħmir diġitali ieħor fin-network tiegħek.

It-tagħmir tiegħek jista' jiġi nfettat mill-malware permezz ta' bosta modi, inklużi:

- żjajjar fuq websajts li jkunu nfettati mill-malware
- tniżżil (downloading) ta' files jew software infettati mill-internet
- ftuħ ta' affarijiet infettati mehmużin ma' imejls.

Ransomware

Ransomware huwa tip komuni u perikoluż ta' malware. Jaħdem billi jsakkarlek jew jaqleb il-files tiegħek f'kodiċi (codes) biex int ma jkunx jista' jkollok aċċess għalihom iktar. Prezz ta' fidwa, normalment f'forma ta' cryptocurrency, jiġi mitlub biex jingħata lura l-aċċess għall-files. Il-persuni kriminali jistgħu ukoll jheddu li jippubblikaw jew ibigħu informazzjoni online, jekk il-prezz mitlub ma jitħallasx.

Modi ta' mitigazzjoni

Waqt li software anti-virus jew ta' sigurtà jista' jgħin biex jipproteġik mill-malware, l-ebda software ma huwa effettiv 100%. L-istaff għandu jkun attent rigward imejls, websajts u tniżżil ta' files, u għandu jaġġorna regolarment it-tagħmir diġitali tiegħu biex jibqa' dejjem sikur.

Ara dawn ir-riżorsi li ġejjin għal iktar informazzjoni dwar il-protezzjoni tan-negozju tiegħek mir-ransomware:

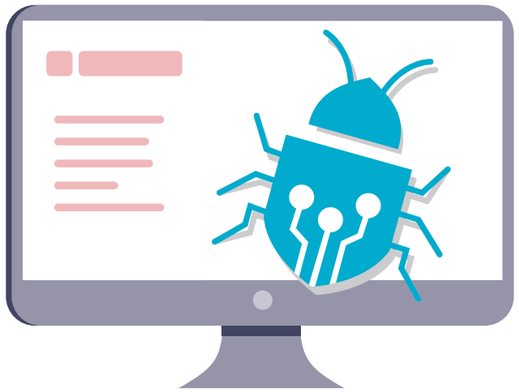
- Ransomware
- Ipproteġi lilek innifsek kontra attakki ta' ransomware
- X'għandek tagħmel jekk tkun vittma ta' domanda għall-fidwa

Studju ta' każ:

Impjegati ta' ħanut tal-parts tal-karozzi waslu għax-xogħol għodwa waħda u ma setgħux iqabbdu s-server tal-kompjuter. Meta l-provveditur tal-IT tagħhom kiseb aċċess għas-server, sabu tieqa miftuħa li kienet tgħid li l-informazzjoni kollha fil-kompjuter kienet ġiet maqluba f'kodiċi. In-nota talbet il-ħlas għall-fidwa f'bitcoin biex il-files jerġgħu jinfetħu.

Kien hemm drive għall-backup imwaħħla ġewwa l-kompjuter, li ukoll kien ġie maqlub f'kodiċi. Huma pruvaw jagħmlu konnessjoni b'iktar drives għall-backup, iżda l-files ġew awtomatikament maqluba f'kodiċi f'sekondi. **Huma ma rnexxielhomx ineħħu r-ransomware qabel ma pruvaw jirkupraw id-data u tilfu kull file b'backup li kellhom.**

L-unika għażla li kien baqa' kien li jerġa jkun issettjat is-server tal-fabbrika mill-ġdid u tibda b'sistema oħra ġdida. In-negozju tilef bosta snin ta' data u kellu jerġa' jibda mill-bidu.



Assigura l-kontijiet tiegħek

Attiva l-awtentikazzjoni multi-fattorali

L-awtentikazzjoni multi-fattorali (MFA) tagħmilha diffiċli għall-persuni kriminali biex jiksbu aċċess għall-kontijiet tiegħek.

MFA żżid saff ieħor ta' sigurtà għall-kont tiegħek. Hija wieħed mill-iktar modi effettivi biex tipproteġi l-kontijiet tiegħek minn xi ħadd biex jikseb aċċess, għalhekk għandek tużaha kull meta huwa possibbli. Kulmin jilloggja fil-kont tiegħek ikollu jipprovdi xi ħaġa oħra barra l-username u l-password tiegħek. Dan jista' jkun kodiċi uniku minn messaġġ b'text jew app ta' awtentikazzjoni. Għal iktar informazzjoni, aqra l-pariri tagħna dwar MFA, li jinsabu fuq **cyber.gov.au/mfa**.

✓ **Attiva l-MFA kull meta huwa possibli, billi tibda bl-iktar kontijiet importanti tiegħek.**

Implimenta kontrolli għall-aċċess

Ir-restrizzjonijiet għall-aċċess jistgħu jillimitaw il-ħsara kkawżata minn inċident tas-sigurtà diġitali.

Il-kontroll tal-aċċess huwa mod kif jiġi limitat l-aċċess għal ċerti files u sistemi. Tipikament, l-istaff ma jkollux bżonn aċċess totali għall-informazzjoni, kontijiet u sistemi kollha ta' negozju. Għandhom ikunu permessi aċċess biss għal dak bżonnjuż biex jaqdu d-dmirijiet tagħhom.

Ir-restrizzjonijiet għall-aċċess jistgħu jgħinu biex jillimitaw il-ħsara kkawżata minn inċident tas-sigurtà diġitali. Per eżempju, jekk kompjuter ta' membru tal-istaff huwa nfettat b'ransomware, b'kontrolli tajba fuq l-aċċess, jista' jkun affetwat biss numru żgħir ta' files flok in-negozju kollu.

✓ **Aċċerta li kull utent (user) ikollu aċċess biss għal dak li għandu bżonn għar-rwol tiegħu.**

Uża passwords u passphrases b'saħħithom

Ipproteġi l-kontijiet tiegħek mill-kriminali b'password jew passphrase sikuri.

Hafna negozji żgħar jiffaċċjaw attakki diġitali minħabba mġieba fqira rigward passwords. Per eżempju, l-użu tal-istess password f'bosta kontijiet. Tista' tuża kemm maniġer tal-passwords kif ukoll passphrases biex toħloq passwords b'saħħithom.

Maniġer tal-passwords jaġixxi bħala kaxxaforti virtwali għall-passwords tiegħek. Tista' tużah biex toħloq u taħżen passwords b'saħħithom u **uniċi** għal kull kont tiegħek. Jekk għandek ħafna kontijiet, dan jelimina l-piż li tiftakar passwords uniċi. Ma jkollokx għalfejn tiftakar il-passwords jew il-kontijiet li jagħmlu magħhom, għax ikun kollox imniżżel fil-maniġer tal-passwords tiegħek.

Għal-kontijiet li inti tilloggja fihom regolarment, jew li minflok ma tridx li taħżinhom f'maniġer tal-passwords, ikkunsidra tuża passphrase bħala l-password tiegħek. Passphrases huma taħlita ta' kliem addoċċ, per eżempju 'kristall basal tafal pretzil'. Dawn huma ta' għajnuna meta tkun trid password sikur li jkun faċli biex tiftakru. Uża taħlita addoċċ ta' erba' jew iktar kelmiet u żommha unika **- tużax l-istess passphrase** għal bosta kontijiet. Għal iktar informazzjoni, aqra l-parir tagħna dwar il-passphrases u maniġers tal-passwords, misjub fuq **cyber.gov.au/passphrases**.

✓ **Uża maniġer tal-passwords biex toħloq u taħżen passwords uniċi għal kull kont importanti tiegħek.**

Immaniġġja kontijiet li jinqassmu m'oħrajn

Il-qsim tal-kontijiet m'oħrajn jista' jikkomprometti s-sigurtà u jagħmilha iktar diffiċli biex issib irkaptu ta' attività malizzjuża.

F'negozju żgħir, jista' jkun hemm raġunijiet validi għaliex l-istaff ikollu bżonn jaqsam kontijiet ma' membri oħra, iżda dan għandu jkun evitat kemm jista' jkun possibbli. Meta bosta impjegati jużaw l-istess kont jista' jkun diffiċli biex issegwi attività passata ta' impjegat/a speċifiku/a u diffiċli iktar biex issib irkaptu tal-persuni kriminali li jkunu daħlu fiha. Sakemm tbiddel il-password, l-impjegati jkunu jistgħu wkoll ikomplu jaċċessaw il-kontijiet anke wara li jkunu ħallew in-negozju.

✓ **Illimita l-użu tal-kontijiet li jinqasmu m'oħrajn u assigura dawk li huma wżati fin-negozju tiegħek.**

Ipproteġi t-tagħmir diġitali u l-informazzjoni tiegħek

Aġġorna s-software tiegħek

Li żżomm is-software tiegħek aġġornat huwa wieħed mill-aħjar modi biex tipproteġi n-negozju tiegħek minn attakk diġitali.

L-aġġornamenti jistgħu jirranġaw żbalji fis-sistema operattiva u software ieħor, sabiex ikun iktar diffiċli għal kriminal biex jidħol fis-sistema. Żbalji ġodda jkunu skoperti 'l ħin kollu, għalhekk tinjorax suġġerimenti ta' aġġornament. Meta taġġorna s-software tiegħek regolarment tkun qiegħed tnaqqas miċ-ċans li persuna kriminali tuża xi djufija komuni biex jopera xi malware u jbagħbaslek fit-tagħmir diġitali tiegħek. Jekk għandek bżonn għajnuna, l-ACSC ippubblika gwida dwar l-aġġornamenti.

Jekk it-tagħmir diġitali jew software huwa qadim iżżejjed, jista' ma jkunx hemm aġġornamenti għalihom. Jekk il-manifattur ikun waqaf milli jissapportja l-prodott permezz ta' aġġornamenti, għandek tikkunsidra ttejjeb dan permezz ta' prodott ġdid biex tibqa' sikur. Eżempji ta' sistemi li m'għadhomx jirċievu aġġornamenti prinċipali huma **l-iPhone 7** u **Microsoft Windows 7.**

Għal iktar informazzjoni aqra l-gwida tagħna dwar l-aġġornamenti, misjuba fuq **cyber.gov.au/updates**.

✓ **Attiva l-aġġornamenti awtomatiċi għat-tagħmir u s-software tiegħek.**

Uża software tas-sigurtà

Software tas-sigurtà bħal protezzjoni tal-antivirus u ransomware jista' jgħin biex jipproteġi t-tagħmir diġitali tiegħek.

Uża software tas-sigurtà biex issib u tneħħi malware mit-tagħmir diġitali tiegħek. Software tal-antivirus jista' jkun issettjat biex jiskrinja regolarment files u programmi suspettużi. Meta tinsab xi theddida, int tirċievi allarm u l-file suspettuż jgħaddi kwarantina jew jitneħħa.

Hafna negozji żgħar jistgħu jużaw **Windows Security** biex jipproteġu lilhom infushom minn viruses u malware. Windows Security huwa parti minn tagħmir b'Windows 10 u Windows 11 u jinkludi protezzjoni b'xejn kontra l-virus u theddid diġitali.

Tista' wkoll tużah biex tattiva fatturi protettivi ta' ransomware fuq it-tagħmir diġitali tiegħek.

Għal prodotti u għażliet alternattivi, aqra l-parir tagħna dwar is-software tal-antivirus, billi tfittex *antivirus* fuq cyber.gov.au.

✓ **Stabbilixxi software ta' sigurtà biex tagħmel skanjar regolari tat-tagħmir diġitali tiegħek.**

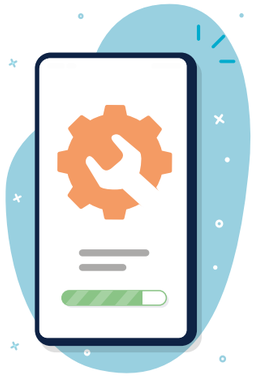
Agħmel back-up tal-informazzjoni tiegħek

Backups regolari jistgħu jgħinuk tirkupra l-informazzjoni tiegħek jekk din tintilef jew tiġi kompromessa.

Il-backup ta' informazzjoni importanti għandha tkun prattika regolari jew awtomatika fin-negozju tiegħek. Mingħajr backup regolari, jista' jkun impossibli għalik biex tirkupra l-informazzjoni tiegħek wara attakk diġitali.

Hemm ħafna metodi u prodotti li tista' tuża biex tagħmel backup tal-informazzjoni tiegħek. Għal parir dettaljat dwar kif tagħmel backup tan-negozju tiegħek, aqra l-parir tagħna dwar backups, misjub fuq **cyber.gov.au/backups**. L-aħjar għażla tvarja skont in-negozju, għalhekk tkellem ma' xi ħadd professjonali fl-IT jekk ma tkunx ċert/a.

✓ **Oħloq u implimenta pjan biex tagħmel backup regolari tal-informazzjoni tiegħek.**



Assigura n-network u s-servizzi esterni tiegħek

Ipproteġi n-negozju tiegħek minn xi attakk diġitali billi tindirizza vulnerabbilitajiet possibbli fin-network tiegħek.

It-tagħmir diġitali u s-servizzi fin-network tiegħek jistgħu jkunu l-mira prinċipali tal-persuni kriminali. Bosta minn dawn is-sistemi jistgħu jkunu kumplessi biex ikunu sikuri, għalhekk iddiskuti r-rakkommandazzjonijiet li ġejjin ma' professjonista tal-IT.

- **Assigura s-servizzi tiegħek:** Jekk tuża NAS jew server ieħor f'darek jew in-negozju tiegħek, ħu iktar prekawzjonijiet biex tassigurahom. Dan it-tagħmir huwa mira komuni għall-kriminali għaliex dan sikwit ikollu maħżun fih files importanti jew ikun jagħmel funzjonijiet importanti. Hemm bosta strateġiji ta' mitigazzjoni meħtieġa għall-protezzjoni ta' dan it-tagħmir. Per eżempju, huwa importanti li wieħed jaċċerta li kull server jew tagħmir NAS ikunu aġġornati regolarment. Kontijiet amministrattivi għandhom ikunu assigurati permezz ta' passphrase f'saħħitha jew awtentikazzjoni multi-fattorali.
- **Naqqas l-attività esterna:** Irrevedi u assigura kull servizz espost għall-internet fin-network tiegħek. Dan jista' jinkludi Desktop Remot, Files maqsuma m'Oħrajn, Webmail u servizzi remoti tal-amministrazzjoni.
- **Emigra għal servizzi tal-cloud:** Ikkunsidra tuża servizzi onlajn jew tal-cloud li joffru sigurtà bħala parti mis-servizz tagħhom, flok ma timmaniġġjaha inti. Per eżempju, uża servizzi onlajn għal affarijiet bħal hosting tal-imejl jew tal-websajt flok ma topera u tassigura dawn is-servizzi inti.
- **Tejjeb is-sigurtà tar-router tiegħek:** Segwi l-gwida tagħna dwar modi biex tassigura r-router tiegħek, inkluż l-aġġornament ta''default passwords', l-użu ta' 'Guest' Wi-Fi għall-klijenti u viżitaturi, u l-użu tal-iktar protokolli f'saħħithom dwar il-qlib tal-informazzjoni f'kodiċi (encryption). Fittex *router* fuq **cyber.gov.au** għal iktar informazzjoni.
- **Ifhem is-sekwenza/katina tal-provvista diġitali tiegħek:** negozji moderni ta' sikwit jingaġġaw bosta servizzi esterni. Per eżempju, fl-użu ta' Managed Service Provider biex imantnu l-IT tagħhom. Problemi ta' sigurtà f'dawn is-servizzi jew provvedituri jistgħu jkollhom impatt sinjifikanti fuq in-negozju tiegħek. Għal parir dettaljat dwar l-immaniġġjar tar-riskju fis-sekwenza tal-provvista diġitali aqra l-Gwida dwar Cyber Supply Chain fuq **cyber.gov.au**.

✓ **Tkellem ma' professjonista tal-IT dwar modi kif tassigura n-network tiegħek.**

Saħħaħ il-websajt tiegħek

Il-websajts huma miri prinċipali tal-attakki diġitali.

Ipproteġi l-websajt tiegħek mill-ħtif billi ssegwi bosta miżuri bażiċi tas-sigurtà:

- assigura l-login tal-websajt tiegħek bl-awtentikazzjoni multi-fattorali jew password f'saħħtu
- aġġorna regolarment is-sistemi tal-immaniġġjar tal-kontenut tal-websajt tiegħek u plugins
- agħmel back-up regolari tal-websajt tiegħek biex tkun tista' ġġeddidha/tirkupraha wara attakk diġitali.

L-ACSC għandu riżorsi addizzjonali għas-sidien tal-websajts. Fittex dawn ir-riżorsi fuq **cyber.gov.au:**

- Akkwisti malajr għall-websajt tiegħek
- Implimentazzjoni taċ-Ċertifikati, TLS, HTTPS u TLS Opportunisti
- Sistema ta' Sigurtà tal-Isem Prinċipali għas-Sidien tas-Sistema Prinċipali
- Preparazzjoni u Reazzjoni għal Attakki ta' Denial-of-Service

✓ **Aqra r-riżorsi tal-ACSC dwar is-sigurtà tal-websajts.**

Issettja mill-ġdid it-tagħmir diġitali tiegħek qabel ma tbiegħu jew tarmih

L-informazzjoni fuq it-tagħmir diġitali qadim tiegħek jista' jkollhom aċċess għaliha persuni stranġieri.

Jekk inti ma tneħħix t-tagħmir diġitali tiegħek b'sigurtà, il-kriminali diġitali jistgħu jiksbu aċċess għall-informazzjoni ta' fuqu. Dan jista' jinkludi imejls, files u informazzjoni oħra rigward negozju. Neħħi l-informazzjoni kollha mit-tagħmir diġitali li jirrigwarda n-negozju tiegħek qabel ma tbiegħu, tpartu jew tarmih. Per eżempju, billi tagħmel issettjar mill-ġdid tal-fabbrika. Dan jgħin biex ineħħi kull informazzjoni u jreġġa' t-tagħmir diġitali għall-issettjar oriġinali tiegħu.

Għal parir dwar l-issettjar mill-ġdid tat-tagħmir diġitali tiegħek, aqra l-parir tagħna dwar kif għandek tneħħi t-tagħmir tiegħek b'sigurtà. Fittex '*dispose*' fuq **cyber.gov.au.**

✓ **Wettaq issettjar mill-ġdid qabel ma tbiegħ jew tarmi tagħmir diġitali tan-negozju.**

Żomm it-tagħmir diġitali tiegħek imsakkar u sigur fiżikament

Restrizzjonijiet fuq l-aċċess għat-tagħmir diġitali tan-negozju jnaqqsu l-opportunitajiet ta' attività malizzjuża.

Limitu tal-aċċess fiżiku għat-tagħmir diġitali tan-negozju tiegħek huwa mod sempliċi biex tevita li informazzjoni tiġi misruqa jew xi attività malizzjuża oħra. Tagħmir diġitali tan-negozju m'għandux jinżamm fejn staff mhux awtorizzat jew membri tal-pubbliku jistgħu jkollhom aċċess għalih.

Uża kontrolli tas-sigurtà biex tipproteġi iżjed it-tagħmir diġitali tiegħek. Ta' l-inqas għandu jkun imsakkar permezz ta' passphrase, PIN jew bijometrika. Aċċerta li t-tagħmir diġitali huwa issettjat biex jissakkar awtomatikament wara perjodu qasir ta' inattività.

✓ **Issettja t-tagħmir diġitali biex jissakkar awtomatikament wara perjodu qasir ta' inattività.**

Ipproteġi l-informazzjoni tiegħek dwar in-negozju

Informazzjoni miżmuma minn negozju tiegħek hija mira attraenti għall-kriminali diġitali.

L-Inċidenti ta' ksur li jirrigwardaw id-dejta qegħdin jiżdiedu - tħallix in-negozju tiegħek jaqa' vittma. Huwa importanti li tifhem x'dejta qed iżomm in-negozju tiegħek, u fejn hija allokata. Meta ssir taf, uża r-rakkommandazzjonijiet f'din il-gwida biex tgħin fil-protezzjoni tal-informazzjoni tiegħek mill-aċċess ta' persuni kriminali. Xi negozji żgħar jista' jkollhom ukoll xi obbligi addizzjonali skont il-liġi.

- **Ikkonsolida l-informazzjoni tan-negozju tiegħek.** Jista' jkun li għandek dejta maħżuna f'ħafna tagħmir diġitali jew servizzi. Meta d-dejta tiġi diċentralizzata, jiżdied in-numru ta' sistemi li jkollok iżżomm sikuri u li jeħtieġu back-up. Sistemi numeruži jistgħu wkoll joħolqu iktar opportunitajiet għal persuni kriminali biex jattakkaw. Fejn huwa possibbli, poġġi l-informazzjoni tan-negozju tiegħek f'post ċentrali li huwa sigur u li jkollu backup regolari. Iċ-ċentralizzazzjoni tal-informazzjoni tiegħek tista' toħloq inċident ta' ksur ikbar jekk is-sistemi tiegħek ikunu kompromessi, għalhekk assigura li dan il-post ċentrali huwa protett adegwatament b'konfigurazzjonijiet sikuri u aċċess restritt. Tkellem ma' professjonist tal-IT jew tas-sigurtà diġitali għal parir.
- **Kun af id-dmirijiet tiegħek tal-protezzjoni tal-informazzjoni.** Xi negozji żgħar jistgħu ikollhom obbligi legali fejn tidħol informazzjoni personali li jżommu. Aqra l-gwida għan-negozji żgħar tal-Uffiċċju tal-Kummissarju Awstraljan tal-Informazzjoni biex titgħallem iktar, fuq **oaic.gov.au**. Ikkonsulta ma professjonista legali jekk m'intix ċert.

✓ **Ifhem id-data miżmuma minn negozju tiegħek u ir-responsabbilitajiet tiegħek biex tipproteġiha.**

Ipprepara lill-impjegati tiegħek

Eduka lill-impjegati

Impjegati bi prattiċi tas-sigurtà diġitali tajbin huma l-ewwel difiża għalik kontra attakki diġitali.

L-impjegati tiegħek għandhom ikollhom għarfien fis-sigurtà diġitali, inkluż is-suġġetti li ġejjin:

- theddid komuni tas-sigurtà diġitali bħal kompromess fl-imejl tan-negozju u ransomware
- miżuri protettivi li jinkludu passwords u passphrases f'saħħithom, MFA u aġġornamenti tas-software
- kif tinduna bi scams u attakki ta' phishing
- politiki speċifiċi għan-negozju (per eżempju, proċessi għar-rapurtar ta' imejls suspettużi jew għall-validazzjoni tal-genwinità tal-fatturi qabel ma jitħallsu)
- x'għandek tagħmel f'emerġenza.

Il-websajt tal-ACSC għandha riżorsi għal biċċa l-kbira ta' dawn is-suġġetti fuq cyber.gov.au/learn. Tista' tikkunsidra wkoll modi oħra kif teduka l-impjegati tiegħek, per eżempju b'kors formali jew taħriġ intern. Tiddeċiedi kif tiddeċiedi, ftakar li t-taħriġ dwar is-sigurtà diġitali mhux meħtieġ darba biss u għandu jkun rivedut perjodikament.

✓ **Iddetermina kif l-għarfien dwar is-sigurtà diġitali se tiġi mgħallma fin-negozju tiegħek.**

Fassal pjan ta' emerġenza

Pjan ta' emerġenza jista' jnaqqas mill-impatt ta' attakk diġitali fuq in-negozju tiegħek.

Meta tirreaġixxi għal inċident tas-sigurtà diġitali, kull minuta tgħodd. Bi pjan ta' emerġenza jfisser li l-istaff tiegħek jista' jieħu inqas ħin biex jifhem x'għandu jagħmel u jkollu iktar ħin biex jieħu azzjoni.

Ikkunsidra l-mistoqsijiet li ġejjin meta tkun qed tfassal il-pjan ta' emerġenza tiegħek:

- X'inhu l-proċess biex l-istaff tiegħek jirraporta inċidenti potenzjali tas-sigurtà diġitali?
- Lil min għandek tikkuntattja għall-għajnuna? Per eżempju, professjonisti tal-IT u l-bank tiegħek.
- L-inċident kif se jiġi kkomunikat lill-istaff tiegħek, persuni b'interessi fin-negozju tiegħek, jew klijenti?
- Kif se timmaniġġja n-negozju bħas-soltu, jekk xi sistemi kritiċi jkunu offlajn?

Assigura li l-istaff tiegħek jiffamiljarizza ruħu mal-pjan tal-emerġenza, inklużi l-irwoli u responsabbilitajiet li jista' jkollhom. Żomm kopja fiżika tal-pjan fil-każ li s-sistemi tiegħek ikunu offlajn meta jkollok bżonnu.

✓ **Oħloq pjan ta' emerġenza għall-inċidenti tas-sigurtà diġitali.**

Żomm ruħek infurmat

Issieħeb mal-ACSC biex tirċievi l-iktar informazzjoni reċenti mill-ACSC.

Żomm ruħek infurmat dwar theddid diġitali u djufijiet l-iktar reċenti billi tissieħeb mal-ACSC. Dan is-servizz jibgħatlek newsletter kull xahar u twissijiet meta theddid diġitali ġdid ikun identifikat.

Is-sigurtà diġitali hija qasam li qiegħed jevolvi b'għaġġla. Il-persuni kriminali jisfruttaw vulnerabbilitajiet b'mod attiv f'temp ta' minuti minn x'ħin jiskopruhom. Meta żżomm ruħek infurmat bil-qasam tas-sigurtà diġitali tkun qed tgħin lin-negozju tiegħek jifhem it-theddid li jista' jkollu jiffaċċja u kif jipproteġi lilu nniffsu kontrihom.

✓ **Irreġistra n-negozju tiegħek mal-Program ta' Sħubija tal-ACSC.**

Għal iktar informazzjoni jew biex tirrapporta inċident tas-sigurtà diġitali, ikkuntattjana:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Dan in-numru jista' jintuża biss fl-Awstralja.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre