Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Panduan keselamatan siber perniagaan kecil-kecilan

Kerumitan Isi Kandungan
MUDAH ●○○

cyber.gov.au

Pengenalan

Bagi sesebuah perniagaan kecil-kecilan, sesuatu insiden keselamatan siber yang kecil sekali pun mungkin akan membawa kesan padah yang hebat. Panduan ini mengandungi langkah-langkah keselamatan asasi bagi membantu anda untuk melindungi perniagaan anda daripada ancaman keselamatan siber yang lazim berlaku. Sebagai permulaan, kami mensyorkan tiga langkah berikut:

- Pasangkan pengesahan pelbagai-faktor
- Kemaskinikan perisian anda
- Buatkan salinan sandaran bagi maklumat anda

Panduan ini mungkin mengandungi langkah-langkah yang tidak relevan kepada perniagaan anda, atau perniagaan anda mungkin mempunyai keperluan yang lebih kompleks. Selepas panduan ini selesai diguna, kami menyarankan agar perniagaan kecil-kecilan menerapkan Maturity Level One (Tahap Kematangan Satu) daripada **Essential Eight** (Lapan Yang Terutama). Jika anda mempunyai sebarang soalan tentang nasihat ini atau keselamatan siber secara umumnya, kami syorkan anda untuk bercakap dengan seorang pakar IT atau penasihat yang dipercayai.

Sila layari cyber.gov.au untuk membaca panduan penuh kami, termasuk nasihat cara bagaimana untuk melakukan setiap langkah berkenaan.

Isi kandungan

Ancaman kepada perniagaan kecil-kecilan

Mesej Scam

Scam merupakan satu cara yang lazim diguna oleh penjenayah siber untuk menyasarkan perniagaan kecil-kecilan. Matlamat mereka adalah untuk menipu anda atau kakitangan anda untuk:

- mengirim wang atau kad hadiah
- klikkan pautan atau lampiran yang berniat jahat
- memberikan maklumat sensitif, seperti kata laluan

Penjenayah siber mungkin akan cuba untuk menipu perniagaan anda melalui e-mel, pesanan ringkas, panggilan telefon dan media sosial. Mereka seringkali akan menyamar sebagai seorang individu atau organisasi yang anda percayai.

Serangan Pancingan (Phishing)

Apa yang membimbangkan khususnya bagi perniagaan kecil-kecilan ialah **serangan pancingan (phishing).** Kaedah penipuan ini sering mengandungi sebuah pautan kepada laman web palsu di mana anda digalakkan untuk mendaftar masuk ke dalam sebuah akaun atau untuk memasukkan butir-butir sulit.

Serangan pancingan biasanya akan mengkompromikan kata laluan akaun anda. Penjenayah siber kerap menggunakan kaedah ini untuk 'mengambilalih' akaun-akaun media sosial perniagaan kecil-kecilan dan memegangnya sebagai tebusan.

Cara untuk memitigasikannya

Jika sesebuah mesej datang daripada sebuah entiti yang dikenali dan kelihatan mencurigakan, berwaspadalah dan berhati-hati. Hubungi orang atau perniagaan berkenaan secara berasingan untuk memeriksa sama ada mesej tersebut sahih atau tidak. Gunakan butir-butir untuk menghubungi mereka yang anda boleh perolehi melalui sebuah sumber yang sahih, misalnya dengan melayari laman web rasmi perniagaan tersebut, dan bukan melalui butir-butir yang terkandung di dalam mesej yang mencurigakan itu**.**

Pelajari cara bagaimana untuk mengenalpasti scam dan serangan pancingan dengan sumber-sumber berikut:

- Kenalpasti dan laporkan scam
- Pelajari cara bagaimana untuk mengenalpasti scam pancingan
- Mengesan mesej-mesej yang Dijana Secara Sosial

Kes contoh:

Seorang pekerja di sebuah syarikat kurier telah menerima sebuah e-mel daripada salah seorang kakitangan eksekutif mereka, yang meminta mereka untuk membeli 6 x $500 kad kredit prabayar. Eksekutif berkenaan telah menyuruh beliau untuk merahsiakan pembelian itu kerana kad-kad ini akan dijadikan baucer hadiah bagi para anggota kakitangan. Setelah ia dibeli, pekerja itu diminta untuk menangkap gambar kedua belah kad-kad tersebut untuk dikirimkan kepada Eksekutif berkenaan sebagai bukti pembeliannya.

Pekerja itu pun melakukan apa yang diarah, dan menggunakan kad kredit peribadi beliau untuk membeli kad-kad hadiah itu di pejabat pos. Beliau menjawab e-mel eksekutif tersebut dan mengirimkan gambar-gambar kad hadiah itu sebagai bukti.

Setelah beliau pulang dari pejabat pos, pekerja itu memberikan kad-kad hadiah yang fizikal itu kepada eksekutif berkenaan – yang tiada tahu-menahu tentang perkara ini. **Selepas semakan dibuat, semua e-mel berkaitan kad-kad hadiah tersebut didapati telah dihantar daripada alamat e-mel rawak dan bukannya daripada akaun e-mel eksekutif itu yang sahih. Ia merupakan sebuah scam semata-mata.**

Serangan e-mel

Selain scam seperti pancingan, satu serangan e-mel yang lazim berlaku ke atas perniagaan kecil-kecilan ialah **business email compromise (kompromi emel perniagaan) (BCE).** Penjenayah boleh menyamar sebagai wakil sesebuah perniagaan dengan menggunakan akaun-akan e-mel yang telah dikompromi, atau melalui kaedah lain – misalnya dengan menggunakan nama domain yang mirip dengan nama sesuatu perniagaan yang sebenar. Selain mencuri maklumat, matlamat serangan ini biasanya ialah untuk menipu mangsa untuk menghantar dana kepada sebuah akaun bank yang diseliakan oleh penipu tersebut.

Cara untuk memitigasikannya

Kaedah pertahanan yang paling baik terhadap serangan emel ialah latihan dan kesedaran kepada pekerja anda. Pastikan kakitangan anda senantiasa berwaspada terhadap emel yang mengandungi perkara berikut:

- permintaan untuk bayaran, khususnya jika ia dikatakan mustahak atau tertunggak
- penukaran butir-butir perbankan
- sebuah alamat e-mel yang tidak kelihatan betul, contohnya nama domain yang tidak sepadan dengan nama syarikat pembekal.

Walaupun serangan ini boleh membawa padah, langkah-langkah pemitigasian mudah dilakukan dan hampir tidak memerlukan sebarang perbelanjaan. **Apabila kakitangan anda menerima e-mel seperti ini, pemitigasian yang paling berkesan ialah untuk memanggil pihak pengirim untuk mengesahkan bahawa mereka benar-benar sahih. Jangan guna butir-butir kontak yang telah dikirimkan kepada anda kerana ia mungkin palsu.** Perkenalkan sebuah proses formal untuk dituruti kakitangan anda bila permintaan bayaran diterima atau butir-butir perbankan ditukar.

Pelajari cara untuk melindungi perniagaan anda daripada scam dan kompromi e-mel BEC dengan sumber-sumber rujukan berikut:

- Pengkompromian emel perniagaan
- Lindungi perniagaan anda daripada penipuan dan pengkompromian emel
- Apa yang perlu dibuat jika perniagaan anda menjadi sasaran penipuan dan pengkompromian emel

Kes Contoh:

Sebuah syarikat pembinaan kecil-kecilan telah menerima sebuah email daripada pembekal mereka yang menyatakan bahawa mereka telah menukar bank mereka. Pihak pembekal tersebut menyampaikan butir-butir akaun baharu mereka untuk pembayaran sebutharga mereka. **Oleh kerana e-mel tersebut kelihatan sahih, syarikat pembinaan itu tidak menelefon pihak pembekal berkenaan untuk mengesahkan perubahan dalam butir-butir akaun perbankan mereka.**

Syarikat tersebut pun membayar sebuah sebutharga daripada pihak pembekal itu yang berjumlah lebih daripada $70,000. Pada keesokan harinya, seorang pekerja lain telah melakukan kesilapan dan telah membayar sebutharga itu sekali lagi dengan bayaran tambahan sebanyak lebih daripada $70,000. Secara keseluruhannya, lebih daripada $150,000 telah dibayar ke dalam akaun bank baharu itu.

Bila syarikat ini menelefon pihak pembekal mereka untuk bertanya jika mereka boleh mengembalikan bayaran yang tersilap itu, pihak pembekal mereka telah menasihatkan bahawa butir-butir perbankan itu ialah salah. Sebuah siasatan langsung dibuat, dan pihak pembekal telah mendapati bahawa salah-satu daripada akaun e-mel mereka telah digodam dan telah menghantarkan butir-butir akaun bank yang palsu. **Tiada dana yang dikembalikan.**

Perisian Berniat Jahat

Perisian Hasad (Malware) ialah takrif umum bagi perisian berniat jahat yang direka untuk menyebabkan kerosakan, misalnya perisian tebusan (ransomware), virus, perisian pengintipan (spyware) dan program pengumpan yang menyamar sebagai program sahih (trojans). Malware boleh:

- mencuri atau mengunci fail-fail dalam alat peranti anda
- mencuri nombor-nombor bank atau kad kredit anda
- mencuri nama pengguna dan kata laluan anda
- mengambil alih kawalan atau mengintip komputer anda.

Malware boleh menghentikan alat peranti anda daripada berfungsi dengan betul, memadam atau mencemarkan fail-fail anda, atau membenarkan pihak lain untuk mengakses maklumat peribadi atau perniagaan anda. Jika alat peranti anda dijangkiti malware, anda mungkin menjadi terdedah kepada serangan lain. Malware tersebut juga boleh merebak kepada alat-alat peranti lain dalam rangkaian jaringan anda.

Alat peranti anda boleh dijangkiti malware melalui beberapa cara, termasuk:

- melawat laman web yang dijangkiti malware
- memuat turun fail-fail atau perisian yang dijangkiti daripada internet
- membuka lampiran e-mel yang dijangkiti

Perisian Tebusan (Ransomware)

Perisian Tebusan (Ransomware) ialah sejenis malware yang lazim ditemui dan berbahaya. Ia berfungsi dengan mengunci atau mempersulitkan (encrypt) fail-fail anda supaya anda tidak boleh mengaksesnya lagi. Sebuah permintaan bayaran tebusan, biasanya dalam bentuk matawang kripto (cryptocurrency), akan dituntut untuk mengembalikan akses kepada fail-fail tersebut. Penjenayah siber juga mungkin akan mengancam untuk menerbitkan atau menjual data anda dalam talian, jika wang tebusan berkenaan tidak dibayar.

Cara untuk memitigasikannya

Walaupun perisian anti-virus atau keselamatan boleh membantu untuk melindungi anda daripada malware, tiada satu pun perisian yang 100% berkesan. Kakitangan anda perlu bersifat peka terhadap e-mel, laman web dan fail-fail yang dimuat turun, dan kerap mengemaskinikan alat-alat peranti mereka untuk mengekalkan keteguhannya.

Sila lihat sumber-sumber rujukan berikut untuk maklumat lanjut tentang cara untuk melindungi perniagaan anda daripada ransomware:

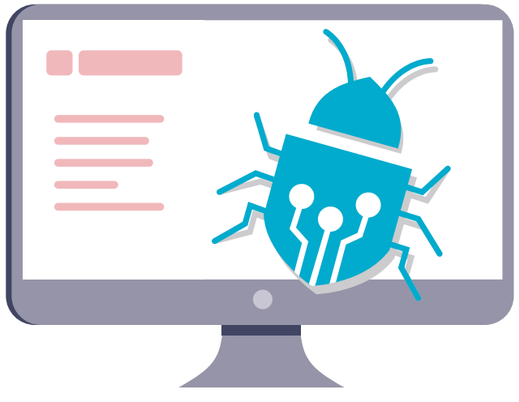
- Ransomware
- Lindungi diri anda daripada serangan ransomware
- Apa yang anda perlu lakukan jika anda dijadikan tebusan

Kes Contoh:

Pekerja sebuah kedai peralatan automobil datang untuk bekerja pada satu pagi dan tidak dapat menghidupkan server komputer mereka. Bila penyedia IT mereka dapat mengakses server tersebut, mereka menemui salah-satu daripada tetingkapnya terbuka dengan sebuah nota yang mengatakan bahawa kesemua data komputer mereka telah dipersulitkan (encrypted). Nota tersebut menuntut mereka membayar pampasan dalam bentuk bitcoin untuk membebaskan kembali fail-fail itu.

Komputer itu mempunyai sebuah pemacu sandaran (backup drive) yang disambung kepadanya, tetapi ia juga telah dipersulitkan. Mereka cuba untuk menyambungkannya kepada pemacu-pemacu sandaran lain, tetapi fail-fail berkenaan terus dipersulitkan sekali secara automatik dalam beberapa saat sahaja. Mereka gagal untul membuang ransomware sebelum melakukan cubaan untuk menyelamatkan data mereka. **Oleh yang demikian mereka pun kehilangan semua fail-fail sandaran yang mereka ada.**

Hanya tinggal satu pilihan sahaja untuk dipertimbangkan iaitu untuk membuat pengembalian ke status kilang (factory reset) dan memulakan kembali dengan sebuah sistem baharu. Syarikat mereka telah mengalami kehilangan data yang dikumpul bertahun-tahun lamanya dan terpaksa mula kembali dengan sepenuhnya.



Teguhkan akaun-akaun anda

Pasangkan pengesahan pelbagai-faktor

Pengesahan pelbagai-faktor (multi-factor authentication) (MFA) menjadikannya lebih sukar bagi penjenayah siber untuk mengakses akaun-akaun anda.

MFA menambah satu lagi lapisan keselamatan ke atas akaun anda. Ia adalah salah-satu daripada cara yang paling berkesan untuk melindungi akaun-akaun anda daripada diakses oleh sesiapa, jadi anda patut menggunakannya bila-bila mungkin. Sesiapa yang mendaftar masuk ke dalam akaun anda akan perlu menyampaikan sesuatu butiran tambahan selain daripada kata pengguna dan kata laluan anda. Ia mungkin mengambil rupa sebuah kod unik daripada sebuah khidmat pesanan ringkas (SMS) atau app pengesahan (authentication app). Untuk maklumat lanjut, sila baca nasihat kami tentang MFA, yang boleh diperolehi di **cyber.gov.au/mfa**.

✓ **Pasangkan MFA bila-bila mungkin, bermula dengan akaun-akaun paling penting anda.**

Terapkan kawalan-kawalan akses

Mengehadkan akses pengguna boleh mengehadkan kerosakan yang disebabkan sebuah insiden keselamatan siber.

Kawalan akses ialah satu cara untuk mengehadkan akses kepada fail-fail dan sistem-sistem tertentu. Biasanya, para kakitangan tidak memerlukan akses sepenuhnya kepada semua data, akaun dan sistem di dalam sesebuah perniagaan. Mereka sepatutnya hanya dibenarkan untuk mengakses apa yang mereka perlukan untuk melakukan tugas-tugas mereka.

Mengehadkan akses akan membantu untuk mengehadkan kerosakan yang disebabkan sebuah insiden serangan siber. Contohnya, jika komputer seseorang kakitangan dijangkiti ransomware, dengan kawalan akses yang sewajarnya, ia mungkin hanya akan menjejaskan sebahagian kecil fail-fail daripada keseluruhan perniagaan itu sendiri.

✓ **Pastikan setiap pengguna hanya boleh mengakses apa yang mereka perlukan untuk peranan mereka.**

Gunakan kata laluan atau frasa laluan yang kuat

Lindungi akaun-akaun anda daripada penjenayah siber dengan sebuah kata laluan atau frasa laluan yang teguh.

Ramai perniagaan kecil-kecil menghadapi serangan siber akibat tingkahlaku kata laluan yang lemah. Contohnya, menggunakan kata laluan yang sama untuk pelbagai akaun. Anda boleh menggunakan kedua-dua pengurus kata laluan (password manager) dan frasa laluan untuk menghasilkan kata laluan yang kuat.

Sebuah **pengurus kata laluan** bertindak seperti sebuah peti besi maya untuk kata-kata laluan anda. Anda boleh menggunakannya untuk menghasilkan dan menyimpan kata laluan yang kuat dan **unik** bagi setiap akaun anda. Jika anda mempunyai banyak akaun, ini akan meringankan beban untuk perlu mengingati kata-kata laluan unik. Anda tidak perlu ingat kata-kata laluan atau akaun-akaun yang memilikinya, kerana semuanya sudah pun dirakamkan dalam pengurus kata laluan anda.

Untuk akaun-akaun yang kerap didaftar masuk oleh anda, atau yang anda tidak mahu simpankan di dalam sebuah pengurus kata laluan, pertimbangkan penggunaan sebuah frasa laluan sebagai kata laluan anda. Frasa laluan adalah sebuah campuran perkataan rawak, contohnya 'kristal bawang tanah liat pretzel'. Ia berguna bila anda mahu sebuah kata laluan teguh yang mudah diingat. Gunakan campuran empat atau lebih perkataan rawak dan pastikan ia unik – **jangan guna kembali sebuah frasa laluan** pada pelbagai akaun. Untuk maklumat lanjut, sila baca nasihat mengenai pengurus frasa laluan dan kata laluan, kami, yang boleh diperolehi di **cyber.gov.au/passphrases**.

✓ **Gunakan sebuah pengurus kata laluan untuk menghasilkan dan menyimpan kata laluan unik bagi setiap akaun penting anda.**

Uruskan akaun-akaun yang dikongsi

Mengongsi akaun boleh mengkompromikan keselamatan dan menjadikannya sukar untuk menjejak kegiatan yang berniat jahat.

Dalam sebuah perniagaan kecil-kecilan, mungkin terdapat sebab-sebab sahih mengapa para kakitangan perlu mengongsi akaun, tetapi ia harus dielakkan sejauh mana yang boleh. Bila pelbagai kakitangan menggunakan akaun sama ia akan menyukarkan penjejakan aktiviti kembali kepada seseorang pekerja tertentu dan lebih sukar pula untuk menjejaki penjenayah siber yang memecah masuk. Kecuali jika anda menukar kata laluan, para pekerja juga boleh terus mengakses akaun-akaun biarpun bila mereka sudah meninggalkan perniagaan anda.

✓ **Hadkan penggunaan akaun yang dikongsi dan teguhkan mana-mana akaun yang digunakan di dalam perniagaan anda.**

Lindungi alat peranti dan maklumat anda

Kemaskinikan perisian anda

Memastikan perisian anda senantiasa dikemaskini ialah salah satu cara yang terbaik untuk melindungi perniagaan anda daripada sebuah serangan siber.

Pengemaskinian boleh membetulkan kecacatan keselamatan di dalam sistem pengoperasian dan perisian lain anda, jadi ia akan menyukarkan penjenayah siber untuk memecah masuk. Kecacatan baharu senantiasa ditemui, jadi jangan abaikan ujaran untuk mengemaskini. Mengemaskinikan perisian anda dengan kerap akan mengurangkan peluang bagi penjenayah siber untuk menggunakan sebuah kelemahan yang diketahui untuk menghidupkan malware atau menggodam alat peranti anda. Jika anda memerlukan bantuan, ACSC telah menerbitkan panduan tentang pengemaskinian.

Jika alat peranti atau perisian anda sudah terlalu tua, pengemaskinian ini mungkin tidak akan disediakan lagi. Jika pengeluarnya telah menghentikan sokongan produk tersebut dengan pengemaskinian, anda harus timbangkan peningkatkan alat peranti anda kepada sebuah produk lebih baharu untuk kekal teguh. Contoh sistem yang tidak menerima pengemaskinian utama lagi ialah **iPhone 7** dan **Microsoft Windows 7.**

Untuk maklumat lanjut, sila baca panduan mengenai pengemaskinian, kami, yang boleh diperolehi dit **cyber.gov.au/updates**.

✓ **Pasangkan pengemaskinian automatik untuk alat peranti dan perisian anda.**

Gunakan perisian keselamatan

Perisian keselamatan seperti perlindungan anti-virus dan perisian tebusan boleh menolong melindungi alat peranti anda.

Gunakan perisian keselamatan untuk mengesan dan membuang malware daripada alat peranti anda. Perisian anti-virus boleh dipasang untuk kerap melakukan imbasan untuk mengesan fail-fail dan program-program yang mencurigakan. Apabila sesuatu ancaman ditemui, anda akan menerima sebuah pemberitahuan amaran dan fail mencurigakan tersebut akan dikuarantin atau dibuang.

Banyak perniagaan kecil-kecilan boleh menggunakan Windows Security untuk melindungi diri mereka daripada virus dan malware. **Windows Security** sudah dipasang siap di dalam alat-alat peranti Windows 10 dan Windows 11 dan mengandungi perlindungan virus dan ancaman secara percuma. Anda juga boleh menggunakannya untuk memasang ciri-ciri perlindungan perisian tebusan dalam alat peranti anda.

Untuk produk-produk dan pilihan-pilihan lain, sila baca nasihat mengenai perisian anti-virus, kami, dengan membuat carian '*antivirus*' di cyber.gov.au

✓ **Pasangkan perisian keselamatan untuk kerap melakukan imbasan lengkap pada alat peranti anda.**

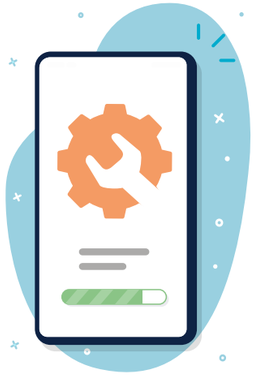
Buatkan salinan sandaran maklumat anda

Salinan sandaran yang kerap dibuat akan membantu anda untuk mengembalikan maklumat anda jika ia hilang atau dikompromi.

Membuat salinan sandaran maklumat penting harus dijadikan satu amalan yang kerap dibuat atau dilakukan secara automatik. Tanpa salinan sandaran yang kerap dibuat, ia mungkin mustahil bagi anda untuk mengembalikan maklumat anda selepas suatu serangan siber.

Terdapat banyak cara dan produk yang anda boleh gunakan untuk membuatkan salinan sandaran maklumat anda. Untuk nasihat terperinci tentang membuat salinan sandaran bagi perniagaan anda, sila baca nasihat untuk membuat salinan sandaran kami, yang boleh diperolehi di **cyber.gov.au/backups.** Pilihan terbaik berbeza bagi setiap perniagaan, jadi bercakaplah dengan seorang profesional IT jika anda tidak pasti.

✓ **Wujudkan dan terapkan sebuah pelan untuk kerap membuat salinan sandaran maklumat anda.**



Teguhkan perkhidmatan sistem jaringan dan luaran anda

Lindungi perniagaan anda daripada serangan siber dengan menangani potensi kelemahan dalam rangkaian jaringan anda.

Alat peranti dan perkhidmatan di dalam rangkaian jaringan anda boleh menjadi suatu sasaran utama bagi penjenayah siber. Kebanyakan sistem ini mungkin rumit untuk diteguhkan, jadi bincangkan saranan-saranan berikut dengan seorang profesional IT.

- **Teguhkan server anda:** Jika anda menggunakan sebuah NAS atau server lain di rumah atau dalam perniagaan anda, ambil langkah berjaga-jaga yang lebih berwaspada untuk meneguhkannya. Alat-alat peranti ini menjadi sasaran biasa bagi penjenayah siber kerana ia sering menyimpan fail-fail penting atau melakukan fungsi penting. Terdapat banyak strategi pemitigasian yang diperlukan untuk melindungi alat-alat peranti ini. Contohnya, ianya penting untuk memastikan agar mana-mana server atau alat peranti NAS kerap dibuat salinan sandaran bagi mereka. Akaun-akaun pentadbiran harus diteguhkan dengan sebuah frasa laluan yang kuat atau pengesahan pelbagai-faktor.

- **Meminimumkan tetapak (footprint) menghadap-ke-luar (external facing):** Audit dan teguhkan mana-mana perkhidmatan yang terdedah kepada internet dalam rangkaian jaringan anda. Ini mungkin termasuk Meja Jarak jauh (Remote Desktop), Perkongsian Fail (File Shares), Webmail dan perkhidmatan pentadbiran jarak jauh.

- **Pindah kepada perkhidmatan awan (cloud services):** Pertimbangkan penggunaan perkhidmatan dalam talian atau awan yang menawarkan keselamatan terbina, daripada menguruskannya dengan sendiri. Contohnya, gunakan perkhidmatan dalam talian untuk perkara-perkara seperti e-mel atau penghosan laman web daripada menjalankan dan meneguhkan perkhidmatan-perkhidmatan ini dengan sendiri.

- **Tingkatkan keselamatan router anda:** Sila turuti panduan kami tentang cara untuk meneguhkan router anda termasuk mengemaskinikan kata laluan alpa, memasang Wi-Fi "Tetamu" ("Guest") untuk pelanggan atau pelawat, dan gunakan protokol penyulitan (encryption) yang paling kuat. Untuk maklumat lanjut, sila buat carian untuk *'router'* di **cyber.gov.au.**

- **Fahami rantaian bekalan siber anda:** Perniagaan moden sering menyumberluarkan pelbagai perkhidmatan. Contohnya, dengan menggunakan sebuah Penyedia Perkhidmatan Terurus (Managed Service Provider) untuk menyelenggarakan IT mereka. Isu-isu keselamatan dengan perkhidmatan atau penyedia ini mungkin akan mempunyai kesan yang signifikan ke atas perniagaan anda. Untuk nasihat terperinci mengenai pengurusan risiko rantaian bekalan siber, sila baca Panduan Rantaian Bekalan Siber kami di **cyber.gov.au**

✓ **Bercakaplah dengan seorang pakar IT tentang cara bagaimana untuk memperkukuhkan sistem jaringan anda.**

Kukuhkan laman web anda

Laman web ialah sasaran utama bagi serangan siber.

Lindungi laman web anda daripada dijadikan tebusan dengan mematuhi beberapa langkah keselamatan asasi:

- teguhkan pendaftaran masuk ke dalam laman web anda dengan pengesahan pelbagai-faktor atau satu kata laluan yang kuat.
- kemaskinikan sistem pengurusan isi kandungan dan plugin laman web anda dengan kerap
- buatkan salinan sandaran bagi laman web anda dengan kerap supaya anda boleh mengembalikannya selepas sesuatu serangan siber.

ACSC mempunyai sumber-sumber rujukan tambahan yang disediakan untuk pemilik laman web. Sila buat carian untuk sumber-sumber rujukan ini di **cyber.gov.au**

- Kejayaan pantas untuk laman web anda
- Terapkan Sijil-Sijil (Certificates), TLS, HTTPS dan Opportunistic TLS.
- Keselamatan Sistem Nama Domain (Domain Name System Security) untuk Pemilik Domain
- Bersiapsiaga untuk dan Merespons kepada Serangan Penafian Perkhidmatan (Denial-of-Service)

✓ **Sila baca sumber-sumber rujukan ACSC mengenai keselamatan laman web.**

Setkan kembali alat-alat peranti anda sebelum ia dijual atau dilupuskan

Data dalam alat peranti lama anda mungkin boleh diakses oleh orang yang anda tidak kenali.

Jika anda tidak melupuskan alat peranti anda dengan selamat, penjenayah siber mungkin boleh mengakses maklumat yang terkandung di dalamnya. Ini mungkin termasuk emel, fail-fail dan data perniagaan anda yang lain. Padamkan semua maklumat daripada alat peranti perniagaan anda sebelum anda menjual, menukar atau melupuskannya. Contohnya, dengan melakukan pengesetan kembali ke status kilang (factory reset). Ini akan menolong anda untuk memadamkan sebarang maklumat yang ada dan mengembalikan alat peranti tersebut kepada status pengesetan asalnya.

Untuk nasihat tentang pengesetan kembali alat peranti anda, sila baca panduan kami tentang cara bagaimana untuk melupuskan alat peranti anda dengan selamat. Sila buat carian untuk *'dispose'* di **cyber.gov.au.**

✓ **Lakukan pengesetan kembali ke status kilang sebelum anda menjual atau melupuskan alat peranti perniagaan anda.**

Kuncikan alat peranti anda dan teguhkan secara fizikal

Mengehadkan akses kepada alat peranti perniagaan anda akan mengurangkan peluang berlakunya kegiatan yang berniat jahat.

Mengehadkan akses fizikal kepada alat peranti perniagaan anda ialah cara mudah untuk menghindarkan data daripada dicuri atau sebarang kegiatan berniat jahat yang lain. Alat peranti perniagaan tidak patut disimpan di tempat di mana kakitangan yang tidak dibenarkan atau orang awam boleh mengaksesnya.

Gunakan kawalan keselamatan untuk melindungi alat-alat peranti perniagaan anda dengan lebih lanjut. Pada kadar seminimumnya, ia patut dikunci dengan sebuah frasa laluan, PIN atau metrik-bio. Pastikan alat-alat peranti ini diset secara automatik untuk dikunci selepas sebuah tempoh masa tanpa aktiviti yang singkat.

✓ **Konfigurasikan alat-alat peranti anda untuk menguncikan diri secara automatik selepas tempoh masa tanpa aktiviti yang singkat.**

Lindungi data perniagaan anda

Data yang dipegang oleh perniagaan anda merupakan sasaran yang menarik kepada penjenayah siber.

Pencerobohan data sedang meningkat – jangan jadikan perniagaan anda mangsanya. Ia penting untuk memahami apa data yang dipunyai perniagaan anda, dan di lokasi apa. Bila anda menyedari akan perkara ini, gunakan saranan-saranan dalam panduan ini untuk membantu melindungi data anda daripada diakses oleh penjenayah siber. Sesetengah perniagaan kecil-kecilan mungkin mempunyai kewajipan tambahan juga di bawah undang-undang.

- **Gabungkan data perniagaan anda.** Anda mungkin ada data yang disimpan di serata tempat dalam pelbagai alat peranti atau perkhidmatan. Bila data dinyahpusatkan (decentralised), ia menggandakan bilangan sistem yang anda perlu teguhkan dan sandarkan. Pelbagai sistem juga boleh mewujudkan lebih banyak peluang bagi sesuatu serangan siber untuk berlaku. Sejauh mana yang boleh, simpankan data perniagaan anda di dalam sebuah lokasi pusat yang teguh dan kerap dibuatkan salinan sandaran. Pemusatan data anda boleh menyebabkan sebuah pencerobohan yang lebih besar jika sistem-sistem anda dikompromi, jadi pastikan lokasi pusat ini dilindungi dengan secukupnya dengan konfigurasi yang teguh dan akses terhad. Bercakaplah dengan seorang profesional IT atau keselamatan siber untuk mendapatkan nasihat.
- **Ketahui kewajipan anda untuk melindungi data.** Sesetengah perniagaan kecil-kecilan mungkin mempunyai kewajipan undang-undang untuk menangani maklumat peribadi yang mereka kumpul. Untuk mendapatkan maklumat lebih lanjut, sila baca Panduan bagi Perniagaan Kecil-Kecilan pihak Pejabat Pesuruhjaya Maklumat Australia (Office of the Australian Information Commissioner) yang boleh diperolehi di **oaic.gov.au.** Rundingkan dengan seorang profesional guaman jika anda tidak pasti.

✓ **Fahami data yang dipegang perniagaan anda dan tanggungjawab anda untuk melindunginya.**

Siapsiagakan kakitangan anda

Didikkan para pekerja anda

Pekerja dengan amalan keselamatan siber yang baik merupakan barisan pertahanan pertama anda dalam melawan serangan siber.

Para pekerja anda harus mempunyai kesedaran mengenai keselamatan siber, termasuk topik-topik berikut:

- ancaman keselamatan siber lazim seperti pengkompromian e-mel perniagaan dan perisian tebusan (ransomware)
- langkah-langkah perlindungan termasuk kata laluan kuat ata frasa laluan, MFA dan pengemaskinian perisian
- Cara bagaimana untuk mengenalpasti scam dan serangan pancingan
- dasar-dasar khusus perniagaan (contohnya, proses-proses untuk melaporkan emel mencurigakan atau untuk menentusahkan sesuatu sebutharga ialah tulen sebelum membayarnya).
- apa yang patut dilakukan dalam sebuah kecemasan.

Laman web ACSC mempunyai sumber-sumber rujukan bagi kebanyakan topik-topik ini di cyber.gov.au/learn. Anda boleh mempertimbangkan kaedah-kaedah lain untuk mendidik para pekerja anda, contohnya melalui sebuah kursus formal atau latihan dalaman. Biar apa pun keputusaan anda, ingatlah bahawa latihan keselamatan siber bukannya satu keperluan yang hanya dilakukan sekali sahaja dan patut disegar semula secara berkala.

✓ **Tentukan cara bagaimana kesedaran keselamatan siber akan diajar di dalam perniagaan anda.**

Buatkan sebuah pelan kecemasan

Sebuah pelan kecemasan boleh mengurangkan kesan sesebuah serangan siber ke atas perniagaan anda.

Setiap minit amat berharga bila merespons kepada sebuah insiden keselamatan siber. Dengan adanya sebuah pelan kecemasan, kakitangan anda tidak perlu membazirkan masa untuk memikirkan apa yang harus dilakukan dan sebaliknya boleh menggunakan masa tersebut untuk mengambil tindakan.

Pertimbangkan soalan-soalan berikut sewaktu merekacipta pelan kecemasan anda:

- Apa proses yang ada bagi kakitangan and untuk melaporkan insiden keselamatan siber yang berpotensi berlaku?
- Siapa yang anda harus hubungi untuk bantuan? Contohnya, profesional IT dan bank anda.
- Bagaimana insiden tersebut akan dimaklumkan kepada kakitangan, pemegang taruh, atau pelanggan anda?
- Bagaimana anda akan menguruskan perniagaan anda seperti biasa, jika terdapat mana-mana sistem kritikal yang tergendala di luar talian?

Pastikan kakitangan anda biasa dengan pelan kecemasan tersebut, termasuk apa-apa peranan atau tanggungjawab yang mereka mungkin ada. Adakan sebuah salinan cetak pelan tersebut jika sistem anda tergendala di luar talian bila anda memerlukannya.

✓ **Wujudkan sebuah pelan kecemasan untuk insiden-insiden keselamatan siber.**

Ketahui perkembangan terkini

Jadilah rakan ACSC untuk menerima maklumat terkini daripada ACSC.

Ketahui maklumat terkini mengenai ancaman siber dan kelemahan dengan menjadi rakan ACSC. Perkhidmatan ini akan menghantar risalah berita bulanan dan amaran pemberitahuan kepada anda bila sesuatu ancaman siber baharu dikenalpasti.

Keselamatan siber ialah sebuah bidang yang cepat berubah. Penjenayah siber mengeksploitasikan kelemahan secara aktif dalam kadar tempoh beberapa minit sesudah ia dikesan mereka sahaja. Mengetahui maklumat terkini tentang landskap keselamatan siber akan membantu perniagaan anda untuk memahami ancaman yang kemungkinan besar akan dihadapinya dan cara bagaimana untuk melindungi diri daripada mereka.

✓ **Daftarkan perniagaan anda dengan Program Perkongsian ACSC (ACSC Partnership Program).**

Penafian

Bahan di dalam panduan ini adalah bersifat umum dan tidak harus dianggap sebagai nasihat perundangan atau digantung sebagai bantuan dalam apa-apa keadaan atau kecemasan tertentu. Dalam sebarang hal mustahak, anda harus mendapatkan nasihat profesional bebas tentang apa yang anda sedang alami sendiri.

Pihak Komanwel tidak menerima tanggungjawab atau tanggungan ke atas sebarang kerosakan, kerugian atau perbelanjaan yang ditanggung akibat daripada pergantungan kepada maklumat yang terkandung dalam panduan ini.

Hakcipta Terpelihara

© Komanwel Australia 2023
Dengan pengecualian Jata Negara dan di mana-mana tempat yang menyatakan sebaliknya, semua bahan yang disampaikan di dalam terbitan ini telah disediakan di bawah lesen Creative Commons Attribution4.0 International (www.creativecommons.org/licenses).

Untuk mengelakkan sebarang keraguan, ini bererti bahawa lesen ini hanya bertakluk ke atas bahan-bahan yang disampaikan di dalam dokumen ini.

Butir-butir syarat-syarat lesen yang berkenaan boleh diperolehi daripada laman web Creative Commons dan begitu juga kod perundangan lengkap bagi lesen CC BY 4.0 (www.creativecommons.org/licenses).

Penggunaan Jata Negara

Terma-terma yang mengawal penggunaan Jata Negara telah dibutirkan di dalam laman web Jabatan Perdana Menteri dan Kabinet (www.pmc.gov.au/government/commonwealth-coat-arms).

Untuk maklumat lanjut, atau untuk melaporkan sebuah insiden keselamatan siber, sila hubungi kami di:

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

Nombor ini tersedia untuk digunakan di dalam Australia sahaja.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre