Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Usaha Kecil panduan keamanan siber

Kompleksitas Konten
SEDERHANA ● ○ ○

cyber.gov.au

Pendahuluan

Untuk usaha kecil, bahkan insiden keamanan siber kecil pun dapat menimbulkan dampak yang menghancurkan. Panduan ini mencakup langkah-langkah keamanan dasar untuk membantu melindungi bisnis Anda dari ancaman keamanan siber yang umum. Sebagai titik awal, kami merekomendasikan tiga langkah berikut:

- Aktifkan autentikasi multifaktor
- Perbarui perangkat lunak Anda
- Cadangkan informasi Anda

Panduan ini mungkin mencakup tindakan yang tidak relevan dengan bisnis Anda, atau bisnis Anda mungkin memiliki kebutuhan yang lebih kompleks. Setelah menyelesaikan panduan ini, kami menyarankan usaha kecil menerapkan Maturity Level One dari Essential Eight. Jika Anda memiliki pertanyaan tentang saran ini atau keamanan siber secara lebih luas, sebaiknya Anda berbicara dengan profesional TI atau penasihat tepercaya.

Kunjungi cyber.gov.au untuk membaca panduan lengkap kami, termasuk saran cara untuk setiap tindakan.

Daftar isi

Ancaman terhadap usaha kecil

Pesan Penipuan

Penipuan adalah cara umum yang dilakukan penjahat dunia maya untuk menargetkan usaha kecil. Tujuan mereka adalah untuk menipu Anda atau staf Anda agar:

- mengirimkan uang atau kartu hadiah
- mengklik tautan atau lampiran berbahaya
- memberikan informasi sensitif, seperti sandi.

Penjahat dunia maya dapat mencoba dan menipu bisnis Anda melalui email, pesan teks, panggilan telepon, dan media sosial. Mereka sering berpura-pura menjadi orang atau organisasi yang Anda percayai.

Serangan phishing

Yang menjadi perhatian khusus bagi usaha kecil adalah **serangan phishing**. Penipuan ini sering kali berisi tautan ke situs web palsu tempat Anda disarankan untuk masuk ke akun atau memasukkan detail rahasia.

Serangan phishing biasanya membahayakan kata sandi akun Anda. Penjahat dunia maya sering menggunakan metode ini untuk "mengambil alih" akun media sosial usaha kecil dan menahannya untuk mendapatkan uang tebusan.

Cara-cara mitigasi

Jika pesan berasal dari entitas yang dikenal dan tampak mencurigakan, berhati-hatilah. Hubungi orang atau bisnis tersebut secara terpisah untuk memeriksa apakah pesan tersebut sah. Gunakan detail kontak yang Anda temukan melalui sumber yang sah, misalnya dengan mengunjungi situs resmi bisnis, dan bukan yang tercantum dalam pesan yang mencurigakan.

Pelajari lebih lanjut cara mengidentifikasi penipuan dan serangan phishing dengan sumber berikut:

- Mengenali dan melaporkan penipuan
- Mempelajari cara mengenali penipuan phishing
- Mendeteksi Pesan yang Direkayasa Secara Sosial.

Studi kasus:

Seorang karyawan di sebuah perusahaan kurir menerima email dari salah satu staf eksekutif mereka, meminta mereka untuk membeli 6 x $500 kartu kredit prabayar MasterCard. Eksekutif menyuruhnya untuk merahasiakannya karena kartu itu akan menjadi voucher hadiah untuk anggota staf. Setelah dibeli, karyawan diminta untuk memotret kedua sisi kartu dan mengirimkannya ke Eksekutif sebagai bukti pembelian.

Seperti yang diinstruksikan, karyawan tersebut pergi ke kantor pos dan menggunakan kartu kredit pribadinya untuk membeli kartu hadiah. Dia membalas email eksekutif dan mengirimkan foto kartu hadiah sebagai bukti.

Setelah kembali dari kantor pos, karyawan tersebut memberikan kartu fisik kepada eksekutif – yang tidak mengetahuinya. Saat ditinjau, **semua email tentang kartu hadiah tersebut berasal dari alamat email acak dan bukan dari akun email resmi eksekutif. Itu adalah penipuan.**

Serangan email

Selain penipuan seperti phishing, serangan email yang umum terhadap usaha kecil adalah **penyusupan email bisnis** (BEC). Penjahat dapat menyamar sebagai perwakilan bisnis dengan menggunakan akun email yang disusupi, atau melalui cara lain – seperti menggunakan nama domain yang terlihat mirip dengan bisnis yang asli. Selain mencuri informasi, tujuan dari serangan ini biasanya untuk menipu korban agar mengirimkan dana ke rekening bank yang dioperasikan oleh penipu tersebut.

Cara-cara mitigasi

Pertahanan terbaik terhadap serangan email adalah pelatihan dan kesadaran bagi karyawan Anda. Pastikan staf Anda mengetahui untuk selalu berhati-hati terhadap email dengan hal-hal berikut:

- permintaan untuk pembayaran, terutama jika mendesak atau lewat waktu
- perubahan rincian bank
- alamat email yang terlihat tidak benar, seperti nama domain yang tidak sama persis dengan nama perusahaan pemasok.

Meskipun serangan-serangan ini dapat menghancurkan, langkah-langkah mitigasinya mudah dan hampir tidak ada biaya. **Saat staf menerima email seperti ini, mitigasi yang paling efektif adalah menelepon pengirim untuk memastikan bahwa email tersebut sah.** Jangan gunakan detail kontak yang telah dikirimkan kepada Anda karena ini bisa jadi penipuan. Perkenalkan proses formal untuk diikuti staf saat permintaan pembayaran diterima atau detail bank diubah.

Pelajari cara melindungi bisnis Anda dari penipuan BEC dan email yang tersusupi dengan sumber berikut:

- Email bisnis yang tersusupi
- Lindungi bisnis Anda dari penipuan dan penyusupan email
- Apa yang harus dilakukan jika bisnis Anda menjadi sasaran penipuan atau penyusupan email.

Studi kasus:

Sebuah bisnis konstruksi kecil menerima email dari pemasok mereka yang mengatakan bahwa mereka telah berganti bank. Pemasok memberikan rincian rekening baru untuk pembayaran tagihan. Karena email tersebut tampak sah, **bisnis konstruksi tidak menghubungi pemasok untuk mengonfirmasi perubahan detail rekening bank.**

Bisnis konstruksi tersebut membayar tagihan dari pemasok sebesar lebih dari $70.000. Keesokan harinya, karyawan lain secara tidak sengaja membayar tagihan yang sama lagi untuk jumlah tambahan di atas $70.000. Secara keseluruhan, lebih dari $150.000 telah dibayarkan ke rekening bank yang baru.

Ketika bisnis konstruksi menelepon pemasok mereka untuk menanyakan apakah mereka dapat mengembalikan pembayaran duplikat, pemasok memberi tahu bahwa rincian perbankan itu salah. Penyelidikan segera diluncurkan, dan pemasok menemukan bahwa salah satu akun email mereka telah diretas dan mengirimkan perincian rekening bank palsu. **Tidak ada dana yang diperoleh kembali.**

Perangkat lunak yang berbahaya

Malware adalah istilah umum untuk perangkat lunak berbahaya yang dirancang untuk menimbulkan bahaya, seperti ransomware, virus, spyware, dan trojan. Malware dapat:

- mencuri atau mengunci berkas di perangkat Anda
- mencuri nomor bank atau kartu kredit Anda
- mencuri nama pengguna dan kata sandi Anda
- mengendalikan atau mematai-matai komputer Anda

Malware dapat menghentikan perangkat Anda agar tidak berfungsi sebagaimana mestinya, menghapus atau merusak berkas Anda, atau memungkinkan orang lain mengakses informasi pribadi atau bisnis Anda. Jika perangkat Anda terinfeksi malware, Anda mungkin rentan terhadap serangan lain. Malware juga dapat menyebar ke perangkat lain di jaringan Anda.

Perangkat Anda dapat terinfeksi oleh malware dalam beberapa cara, termasuk:

- mengunjungi situs web yang telah terinfeksi malware
- mengunduh berkas atau perangkat lunak yang terinfeksi dari internet
- membuka lampiran email yang terinfeksi.

Ransomware

Ransomware adalah jenis perangkat lunak perusak yang umum dan berbahaya. Cara kerjanya yaitu mengunci atau mengenkripsi berkas Anda sehingga Anda tidak dapat mengaksesnya lagi. Uang tebusan, biasanya dalam bentuk mata uang kripto, diminta untuk memulihkan akses ke berkas. Penjahat dunia maya juga dapat mengancam untuk menerbitkan atau menjual data secara online, kecuali jika uang tebusan dibayarkan.

Cara-cara mitigasi

Meskipun perangkat lunak antivirus atau keamanan dapat membantu melindungi Anda dari perangkat malware, tidak ada perangkat lunak yang 100% efektif. Staf harus waspada dengan email, situs web, dan unduhan berkas, serta memperbarui perangkat mereka secara berkala agar tetap aman.

Lihat sumber daya berikut untuk informasi lebih lanjut tentang cara melindungi bisnis Anda dari ransomware:

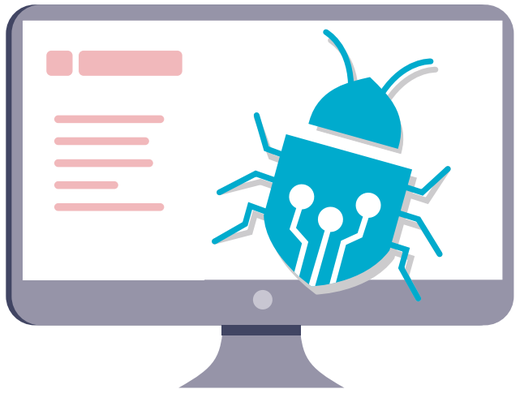
- Ransomware
- Lindungi diri Anda dari serangan ransomware
- Apa yang harus dilakukan jika Anda dimintai tebusan.

Studi kasus:

Karyawan toko onderdil mobil masuk kerja pada suatu pagi dan tidak dapat melakukan boot pada komputer server mereka. Ketika penyedia TI mereka mendapat akses ke server, mereka menemukan jendela terbuka yang mengatakan semua data komputer telah dienkripsi. Catatan itu menuntut mereka membayar uang tebusan dalam bitcoin untuk membuka berkas-berkas yang terkunci.

Ada drive cadangan yang dicolokkan ke komputer, yang juga telah dienkripsi. Mereka mencoba menyambungkan lebih banyak drive cadangan, tetapi berkas-berkas itu secara otomatis dienkripsi dalam beberapa detik. **Mereka gagal menghapus ransomware sebelum mencoba memulihkan data mereka dan kehilangan setiap berkas cadangan yang mereka miliki.**

Satu-satunya pilihan yang tersisa adalah mengatur ulang server ke setelan pabrik dan memulai dari awal dengan sistem yang baru. Bisnis mereka kehilangan data selama bertahun-tahun dan harus memulai dari awal.



Amankan akun Anda

Aktifkan autentikasi multifaktor

Autentikasi multifaktor (Multi-factor Authentication - MFA) mempersulit penjahat dunia maya untuk mengakses akun Anda.

MFA menambahkan lapisan keamanan bagi akun Anda. Ini adalah salah satu cara paling efektif untuk melindungi akun Anda dari seseorang yang ingin mendapatkan akses, jadi Anda harus menggunakannya jika memungkinkan. Siapa pun yang masuk ke akun Anda perlu memberikan hal lain selain nama pengguna dan kata sandi Anda. Ini bisa berupa kode unik dari pesan singkat atau SMS atau aplikasi autentikator. Untuk informasi selengkapnya, baca saran tentang MFA kami, tersedia di **cyber.gov.au/mfa**.

✓ **Nyalakan MFA jika memungkinkan, dimulai dengan akun-akun Anda yang paling penting.**

Menerapkan kontrol akses

Membatasi akses pengguna dapat membatasi kerusakan yang disebabkan oleh insiden keamanan siber.

Kontrol akses adalah cara untuk membatasi akses ke berkas dan sistem tertentu. Biasanya, staf tidak memerlukan akses penuh ke semua data, akun, dan sistem dalam bisnis. Mereka seharusnya hanya diizinkan untuk mengakses apa yang mereka butuhkan untuk melakukan tugas mereka.

Membatasi akses akan membantu membatasi kerusakan yang disebabkan oleh insiden keamanan siber. Misalnya, jika komputer anggota staf terinfeksi ransomware, dengan kontrol akses yang tepat, hal itu mungkin hanya memengaruhi sejumlah kecil berkas daripada usaha secara keseluruhan.

✓ **Pastikan setiap pengguna hanya dapat mengakses apa yang mereka butuhkan untuk peran mereka.**

Gunakan kata sandi atau frasa sandi yang kuat

Lindungi akun Anda dari penjahat dunia maya dengan kata sandi atau frasa sandi yang aman.

Banyak usaha kecil menghadapi serangan siber sebagai akibat dari perilaku kata sandi yang buruk. Misalnya, menggunakan kembali kata sandi yang sama di beberapa akun. Anda dapat menggunakan pengelola kata sandi dan frasa sandi untuk membuat kata sandi yang kuat.

Pengelola kata sandi berfungsi seperti brankas virtual untuk kata sandi Anda. Anda dapat menggunakannya untuk membuat dan menyimpan kata sandi yang kuat dan **unik** untuk setiap akun Anda. Jika Anda memiliki banyak akun, ini menghilangkan beban mengingat kata sandi yang unik. Anda tidak perlu mengingat kata sandi atau akun miliknya, karena semuanya tercatat di pengelola kata sandi Anda.

Untuk akun yang sering Anda gunakan, atau yang tidak ingin Anda simpan di pengelola kata sandi, pertimbangkan untuk menggunakan frasa sandi sebagai kata sandi Anda. Frasa sandi adalah kombinasi dari kata-kata acak, misalnya 'pretzel tanah liat bawang kristal'. Ini berguna saat Anda menginginkan kata sandi aman yang mudah diingat. Gunakan campuran acak dari empat kata atau lebih dan pertahankan agar tetap unik – **jangan gunakan kembali frasa sandi** di beberapa akun. Untuk informasi lebih lanjut, baca baca saran kami tentang frasa sandi dan pengelola kata sandi, tersedia di **cyber.gov.au/passphrases**.

✓ **Gunakan pengelola kata sandi untuk membuat dan menyimpan kata sandi unik untuk setiap akun penting Anda.**

Kelola akun bersama

Berbagi akun dapat mengganggu keamanan dan mempersulit pelacakan aktivitas yang berbahaya.

Dalam usaha kecil, mungkin ada alasan yang sah mengapa staf perlu berbagi akun, tetapi hal ini harus dihindari sebisa mungkin. Ketika beberapa staf menggunakan akun yang sama, akan sulit untuk melacak aktivitas kembali ke karyawan tertentu dan bahkan lebih sulit lagi untuk melacak penjahat dunia maya yang masuk. Kecuali Anda mengubah kata sandi, karyawan juga dapat terus mengakses akun bahkan setelah mereka meninggalkan bisnis.

✓ **Batasi penggunaan akun bersama dan amankan semua yang digunakan dalam bisnis Anda.**

Lindungi perangkat dan informasi Anda

Perbarui perangkat lunak Anda

Menjaga agar perangkat lunak Anda selalu mutakhir adalah salah satu cara terbaik untuk melindungi bisnis Anda dari serangan dunia maya.

Pembaruan dapat memperbaiki kelemahan keamanan pada sistem operasi Anda dan perangkat lunak lain, sehingga lebih sulit bagi penjahat dunia maya untuk menerobos masuk. Kelemahan baru selalu ditemukan, jadi jangan abaikan permintaan untuk memperbarui. Memperbarui perangkat lunak Anda secara teratur akan mengurangi kemungkinan penjahat dunia maya menggunakan kelemahan yang telah diketahui untuk menjalankan malware atau meretas perangkat Anda. Jika Anda memerlukan bantuan, ACSC telah menerbitkan panduan tentang pembaruan.

Jika perangkat atau perangkat lunak Anda terlalu tua, pembaruan mungkin tidak tersedia. Jika produsen telah berhenti mendukung pembaruan untuk produk itu, Anda harus mempertimbangkan untuk meningkatkan ke produk yang lebih baru agar tetap aman. Contoh sistem yang tidak lagi menerima pembaruan besar adalah **iPhone 7** dan **Microsoft Windows 7**.

Untuk informasi lebih lanjut, baca panduan tentang pembaruan kami, tersedia di **cyber.gov.au/updates**.

✓ **Aktifkan pembaruan otomatis untuk perangkat dan perangkat lunak Anda.**

Gunakan perangkat lunak keamanan

Perangkat lunak keamanan seperti perlindungan antivirus dan ransomware dapat membantu melindungi perangkat Anda.

Gunakan perangkat lunak keamanan untuk mendeteksi dan menghapus malware dari perangkat Anda. Perangkat lunak antivirus dapat diatur untuk memindai berkas dan program yang mencurigakan secara teratur. Saat ancaman ditemukan, Anda akan menerima peringatan dan file yang mencurigakan akan dikarantina atau dihapus.

Banyak usaha kecil dapat **menggunakan Windows Security** untuk melindungi diri dari virus dan malware. Windows Security sudah terpasang di perangkat Windows 10 dan Windows 11 serta mencakup perlindungan virus dan ancaman secara gratis. Anda juga dapat menggunakannya untuk mengaktifkan fitur perlindungan ransomware di perangkat Anda.

Untuk produk dan opsi alternatif, baca saran kami tentang perangkat lunak antivirus, dengan menelusuri *antivirus* di cyber.gov.au.

✓ **Siapkan perangkat lunak keamanan untuk menyelesaikan pemindaian rutin pada perangkat Anda.**

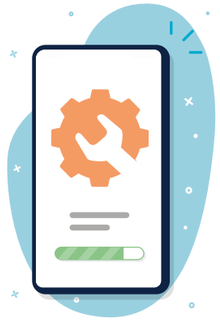
Cadangkan informasi Anda

Pencadangan rutin dapat membantu Anda memulihkan informasi jika hilang atau tersusupi.

Mencadangkan informasi penting harus menjadi praktik rutin atau otomatis dalam bisnis Anda. Tanpa cadangan reguler, tidak mungkin Anda memulihkan informasi setelah serangan dunia maya.

Ada banyak metode dan produk yang dapat Anda gunakan untuk mencadangkan informasi Anda. Untuk saran terperinci tentang mencadangkan bisnis Anda, baca saran kami untuk pencadangan, tersedia di **cyber.gov.au/backups**. Pilihan terbaik akan berbeda-beda untuk setiap bisnis, jadi bicaralah dengan profesional TI jika Anda tidak yakin.

✓ **Buat dan terapkan rencana untuk mencadangkan informasi Anda secara teratur.**



Amankan jaringan dan layanan eksternal Anda

Lindungi bisnis Anda dari serangan dunia maya dengan mengatasi potensi kerentanan di jaringan Anda.

Perangkat dan layanan di jaringan Anda dapat menjadi target utama penjahat dunia maya. Banyak dari sistem ini yang rumit untuk diamankan, jadi diskusikan rekomendasi berikut dengan profesional TI.

- **Amankan server Anda**: Jika Anda menggunakan NAS atau server lain di rumah atau bisnis Anda, berhati-hatilah untuk mengamankannya. Perangkat ini adalah target umum penjahat dunia maya karena sering kali menyimpan berkas penting atau menjalankan fungsi penting. Ada banyak strategi mitigasi yang diperlukan untuk melindungi perangkat ini. Misalnya, penting untuk memastikan server atau perangkat NAS apa pun diperbarui secara rutin. Akun administratif harus diamankan dengan frasa sandi yang kuat atau autentikasi multifaktor.
- **Minimalkan jejak ke luar**: Audit dan amankan semua layanan yang terpapar internet di jaringan Anda. Ini mungkin termasuk Remote Desktop, File Shares, Webmail dan layanan administrasi jarak jauh.
- **Migrasi ke layanan cloud:** Pertimbangkan untuk menggunakan layanan online atau layanan awan yang menawarkan keamanan bawaan, daripada mengelola sendiri. Misalnya, gunakan layanan online untuk hal-hal seperti email atau hosting situs web daripada menjalankan dan mengamankan layanan ini sendiri.
- **Tingkatkan keamanan router Anda:** Ikuti panduan kami tentang cara mengamankan router Anda, termasuk memperbaruikata sandi bawaan, mengaktifkan Wi-Fi "Tamu" untuk pelanggan atau pengunjung, dan menggunakan protokol enkripsi terkuat. Cari *router* di **cyber.gov.au** untuk informasi lebih lanjut.
- **Pahami rantai pasokan dunia maya Anda:** Bisnis modern sering mengalihdayakan beberapa layanan. Misalnya, menggunakan Penyedia Layanan Terkelola untuk memelihara TI mereka. Masalah keamanan pada layanan atau penyedia ini dapat berdampak signifikan pada bisnis Anda. Untuk saran mendetail tentang manajemen risiko rantai pasokan dunia maya, baca Panduan Rantai Pasokan Dunia Maya kami di **cyber.gov.au**.

✓ **Bicaralah dengan profesional TI tentang cara mengamankan jaringan Anda.**

Perkuat situs web Anda

Situs web adalah target utama serangan dunia maya.

Lindungi situs web Anda dari pembajakan dengan mengikuti beberapa tindakan keamanan dasar:

- amankan login situs web Anda dengan autentikasi multifaktor atau kata sandi yang kuat
- perbarui plugin dan sistem manajemen konten situs web Anda secara teratur
- cadangkan situs web Anda secara rutin agar Anda dapat memulihkannya setelah serangan dunia maya.

ACSC memiliki sumber tambahan yang tersedia untuk pemilik situs web. Cari referensi ini di **cyber.gov.au**:

- Quick Wins untuk Situs Web Anda
- Mengimplementasikan Sertifikat, TLS, HTTPS, dan TLS Oportunistik
- Keamanan Sistem Nama Domain untuk Pemilik Domain
- Menyiapkan dan Menanggapi Serangan Denial-of-Service

✓ **Baca sumber daya ACSC tentang keamanan situs web.**

Atur ulang perangkat Anda sebelum dijual atau dibuang

Data di perangkat lama Anda dapat diakses oleh orang asing.

Jika Anda tidak membuang perangkat Anda dengan aman, penjahat dunia maya dapat mengakses informasi di dalamnya. Ini bisa termasuk email, berkas, dan data bisnis lainnya. Hapus semua informasi dari perangkat bisnis Anda sebelum dijual, diperdagangkan atau dibuang. Misalnya dengan melakukan factory reset. Ini akan membantu menghapus semua informasi dan mengembalikan perangkat ke pengaturan aslinya.

Untuk saran tentang menyetel ulang perangkat, baca panduan kami tentang cara membuang perangkat dengan aman. Cari *buang* pada **cyber.gov.au**.

✓ **Lakukan pengaturan ulang pabrik sebelum menjual atau membuang perangkat bisnis.**

Jaga agar perangkat Anda tetap terkunci dan aman secara fisik

Membatasi akses ke perangkat bisnis Anda akan mengurangi peluang untuk aktivitas berbahaya.

Membatasi akses fisik ke perangkat bisnis Anda adalah cara sederhana untuk mencegah data dicuri atau aktivitas berbahaya lainnya. Perangkat bisnis tidak boleh disimpan di tempat yang dapat diakses oleh staf atau khalayak umum yang tidak berwenang.

Gunakan kontrol keamanan untuk melindungi perangkat bisnis Anda lebih lanjut. Setidaknya, perangkat-perangkat tersebut harus dikunci dengan frasa sandi, PIN, atau biometrik. Pastikan perangkat ini diatur untuk mengunci secara otomatis setelah beberapa saat tidak aktif.

✓ **Konfigurasikan perangkat agar terkunci secara otomatis setelah tidak aktif dalam waktu singkat.**

Lindungi data bisnis Anda

Data yang dimiliki oleh bisnis Anda merupakan target yang menarik bagi penjahat dunia maya.

Pelanggaran data terus meningkat – jangan biarkan bisnis Anda menjadi korban. Penting untuk memahami data apa yang dimiliki bisnis Anda, dan di lokasi mana. Setelah Anda mengetahuinya, gunakan rekomendasi dalam panduan ini untuk membantu melindungi data Anda agar tidak diakses oleh penjahat dunia maya. Beberapa usaha kecil mungkin juga memiliki kewajiban tambahan berdasarkan undang-undang.

- **Konsolidasikan data bisnis Anda.** Anda mungkin memiliki data yang tersimpan di berbagai perangkat atau layanan. Ketika data didesentralisasi, ini meningkatkan jumlah sistem yang harus Anda jaga agar tetap aman dan dicadangkan. Banyak sistem juga dapat menciptakan lebih banyak peluang bagi penjahat dunia maya untuk menyerang. Jika memungkinkan, simpan data bisnis Anda di lokasi terpusat yang aman dan dicadangkan secara rutin. Memusatkan data Anda dapat menciptakan pelanggaran yang lebih besar jika sistem Anda disusupi, jadi pastikan lokasi pusat ini terlindungi secara memadai dengan konfigurasi yang aman dan akses terbatas. Bicaralah dengan profesional TI atau keamanan siber untuk mendapatkan saran.
- **Ketahui kewajiban Anda dalam melindungi data.** Beberapa usaha kecil mungkin memiliki kewajiban hukum untuk menangani informasi pribadi yang mereka kumpulkan. Baca panduan untuk usaha kecil Kantor Komisaris Informasi Australia untuk mempelajari lebih lanjut, tersedia di **oaic.gov.au**. Berkonsultasilah dengan pakar hukum jika Anda tidak yakin.

✓ **Pahami data bisnis Anda dan tanggung jawab Anda untuk melindunginya.**

Persiapkan staf Anda

Mendidik karyawan

Karyawan dengan praktik keamanan siber yang baik adalah garis pertahanan pertama Anda melawan serangan siber.

Karyawan Anda harus memiliki kesadaran tentang keamanan siber, termasuk topik-topik berikut:

- ancaman keamanan siber umum seperti penyusupan email bisnis dan ransomware
- langkah-langkah perlindungan termasuk kata sandi atau frasa sandi yang kuat, MFA, dan pembaruan perangkat lunak
- cara mengenali penipuan dan serangan phishing
- kebijakan khusus bisnis (misalnya, proses untuk melaporkan email yang mencurigakan atau untuk memvalidasi faktur asli sebelum membayar)
- apa yang harus dilakukan dalam keadaan darurat.

Situs web ACSC memiliki sumber daya untuk sebagian besar topik ini di cyber.gov.au/learn. Anda mungkin mempertimbangkan cara-cara lain untuk mendidik karyawan Anda, misalnya dengan kursus formal atau pelatihan internal. Apa pun keputusan Anda, ingatlah bahwa pelatihan keamanan siber bukanlah persyaratan sekali pakai dan harus diperbarui secara berkala.

✓ **Tentukan bagaimana kesadaran keamanan siber akan diajarkan dalam bisnis Anda.**

Buat rencana darurat

Rencana darurat dapat mengurangi dampak serangan dunia maya pada bisnis Anda.

Saat menanggapi insiden keamanan siber, setiap menit diperhitungkan. Memiliki rencana darurat berarti staf Anda dapat menghabiskan lebih sedikit waktu untuk memikirkan apa yang harus dilakukan dan lebih banyak waktu untuk bertindak.

Pertimbangkan pertanyaan-pertanyaan berikut saat membuat rencana darurat Anda:

- Apakah proses bagi staf Anda untuk melaporkan potensi insiden keamanan siber?
- Siapa yang Anda hubungi untuk meminta bantuan? Misalnya, profesional TI dan bank Anda.
- Bagaimana insiden tersebut akan dikomunikasikan kepada staf, pemangku kepentingan, atau pelanggan Anda?
- Bagaimana Anda akan mengelola bisnis seperti biasa, jika ada sistem penting yang offline?

Pastikan staf Anda memahami rencana darurat, termasuk peran atau tanggung jawab apa pun yang mungkin mereka miliki. Simpan hard copy rencana itu jika seandainya sistem Anda sedang offline saat Anda membutuhkannya.

✓ **Buat rencana darurat untuk insiden keamanan siber.**

Perbarui informasi

Jadilah mitra ACSC untuk menerima informasi terbaru dari ACSC.

Perbarui informasi tentang ancaman dan kerentanan dunia maya terkini dengan menjadi mitra ACSC. Layanan ini akan mengirimkan kepada Anda buletin bulanan dan peringatan saat teridentifikasi ancaman dunia maya baru.

Keamanan dunia maya adalah bidang yang berkembang pesat. Penjahat dunia maya secara aktif mengeksploitasi kerentanan dalam beberapa menit setelah penemuan mereka. Perbarui informasi tentang lanskap keamanan siber akan membantu bisnis Anda memahami ancaman yang mungkin dihadapi dan cara melindunginya.

✓ **Daftarkan bisnis Anda dengan ACSC Partnership Program.**

Penafian

Materi dalam panduan ini bersifat umum dan tidak boleh dianggap sebagai nasihat hukum atau diandalkan untuk bantuan dalam keadaan tertentu atau situasi darurat. Dalam masalah penting apa pun, Anda harus mencari nasihat profesional independen yang sesuai sehubungan dengan keadaan Anda sendiri.

Persemakmuran tidak bertanggung jawab atau berkewajiban atas kerusakan, kerugian, atau biaya apa pun yang ditimbulkan sebagai akibat mengandalkan informasi yang terkandung dalam panduan ini.

Untuk informasi lebih lanjut, atau untuk melaporkan insiden keamanan siber, hubungi kami:

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

Nomor ini hanya dapat digunakan di Australia.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre