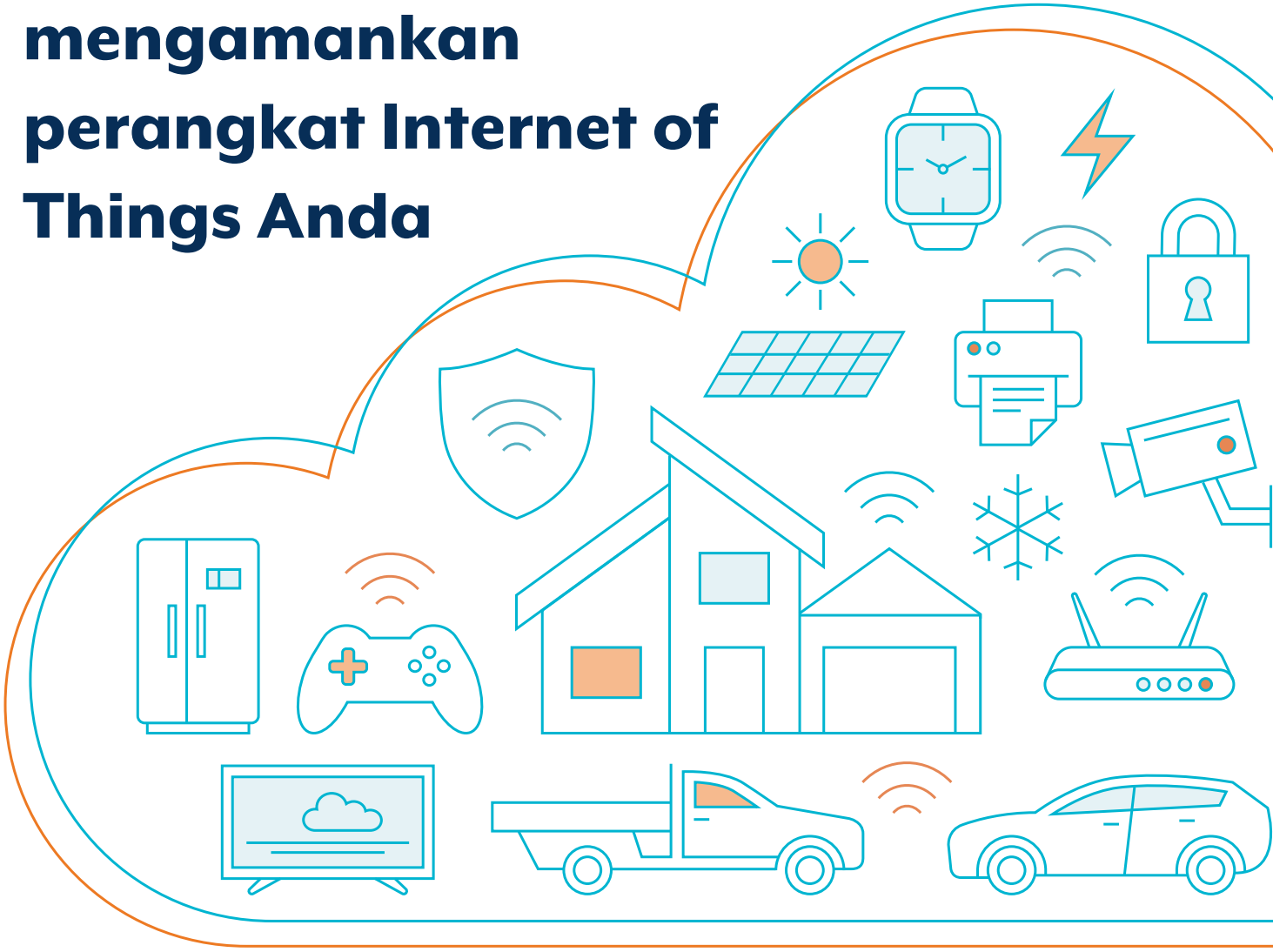
Beberapa tip untuk mengamankan perangkat Internet of Things Anda



Pusat Keamanan Siber Australia telah mengembangkan informasi ini untuk membantu masyarakat membeli dan menggunakan perangkat Internet of Things (IoT) dengan aman. Perangkat IoT adalah barang sehari-hari yang telah terhubung dengan internet. Contoh perangkat IoT antara lain monitor bayi, drone, kamera keamanan, televisi pintar, dan inverter surya. Perangkat IoT di rumah dan bisnis umumnya menggunakan Wi-Fi atau jaringan seluler, seperti 4G atau 5G, untuk terhubung ke internet.

Banyak perangkat IoT yang umum ditemukan di rumah dan bisnis di Australia belum dirancang dengan mempertimbangkan keamanan. Hal ini mengakibatkan perangkat rentan terhadap penyusupan melalui internet. Insiden semacam itu dapat memungkinkan penjahat siber mengakses perangkat dan data pribadi Anda secara tidak sah untuk tujuan jahat.

Sebelum membeli perangkat IoT

Penting untuk meneliti perangkat sebelum membeli, karena produsen menyediakan berbagai tingkat keamanan. Sebelum membeli perangkat, bandingkan perangkat serupa yang dijual oleh berbagai produsen. Hal-hal yang perlu dipertimbangkan antara lain:

1. **Apakah perangkat tersebut dibuat oleh perusahaan ternama dan bereputasi baik serta dijual oleh toko ternama dan bereputasi baik?** Perusahaan ternama dan bereputasi baik cenderung memproduksi perangkat dengan mengutamakan keamanan. Toko ternama dan bereputasi baik cenderung hanya menjual perangkat dari perusahaan ternama dan bereputasi baik, dan memiliki rantai pasokan yang lebih ketat untuk memastikan perangkat sampai ke tangan Anda sesuai dengan yang diinginkan produsen.

2. **Apakah mungkin untuk mengubah kata sandi?**Mengubah kata sandi Anda selalu merupakan hal yang baik. Namun, jika perangkat dikirimkan dengan kata sandi bawaan yang lemah, hal ini menjadi lebih penting. Perangkat dengan keamanan yang baik harus memiliki kata sandi yang unik, tidak dapat diprediksi, rumit, dan tidak dapat ditebak, karena kata sandi bawaan yang lemah adalah cara termudah untuk menyerang perangkat.

3. **Apakah produsen menyediakan pembaruan?** Penting bagi perusahaan untuk menawarkan pembaruan guna memperbaiki kerentanan perangkat segera setelah ditemukan. Misalnya, jika perangkat lunak pada perangkat mengandung kerentanan yang diketahui atau penyusup mengembangkan cara baru untuk menyusupi perangkat Anda, pembaruan diperlukan untuk menyediakan perbaikan.

4. **Data apa yang akan dikumpulkan perangkat dan dengan siapa data tersebut akan dibagikan?** Informasi tentang data apa yang akan dikumpulkan dan bagaimana data tersebut akan digunakan harus tersedia di situs web produsen atau dalam kebijakan privasi mereka. Penting untuk selalu mempertimbangkan informasi yang dikumpulkan oleh aplikasi daring atau seluler.

5. **Apakah perangkat hanya melakukan apa yang Anda inginkan?** Membeli perangkat yang melakukan lebih dari yang Anda butuhkan, termasuk terhubung ke internet, dapat mengurangi keamanan Anda. Kemampuan perangkat yang tidak akan Anda gunakan dapat meningkatkan kerentanan perangkat terhadap serangan tanpa memberikan manfaat apa pun bagi Anda.

Perangkat IoT

Ingatlah beberapa pertanyaan sederhana saat menyiapkan perangkat Anda untuk membantu menjaga jaringan dan data Anda tetap aman.

1. **Apakah perangkat perlu terhubung ke internet?** Hanya karena bisa terhubung, bukan berarti harus terhubung. Perangkat yang tidak terhubung ke internet jauh lebih kecil kemungkinannya untuk disusupi. Jika Anda tidak akan menggunakan fitur yang memerlukan koneksi internet, pertimbangkan apakah perangkat perlu terhubung.

2. **Apakah perangkat berada di lokasi yang aman?** Jika perangkat tidak perlu dipasang di area yang tidak aman, memasangnya di lokasi yang aman dapat mengurangi risiko penyusupan fisik.

3. **Apakah saya perlu mengubah nama pengguna dan kata sandi bawaan?** Penting bagi Anda untuk menggunakan kata sandi atau frasa sandi yang kuat. Jika perangkat Anda tidak dilengkapi dengan kata sandi yang unik, tidak dapat diprediksi, rumit, dan tidak dapat ditebak, kata sandi ini perlu diubah. Nama pengguna dan kata sandi bawaan dikumpulkan dan diunggah secara daring, sehingga perangkat Anda rentan.

4. Apakah **jaringan Wi-Fi saya diatur dengan aman, dan apakah jaringan tersebut memiliki kata sandi yang aman?** Amankan jaringan Wi-Fi dan router Anda agar penyerang lebih sulit mengakses perangkat dan jaringan Anda.

Berikan upaya ekstra

Siapkan jaringan Wi-Fi tambahan di router Anda hanya untuk perangkat IoT. Ini mungkin dikenal di router Wi-Fi Anda sebagai jaringan 'tamu'. Jika perangkat IoT Anda tidak memerlukan komunikasi satu sama lain, aktifkan fitur 'isolasi klien'. Menjaga perangkat IoT Anda tetap terisolasi dari data sensitif memastikan bahwa perangkat IoT yang disusupi tidak memberikan akses ke perangkat atau data Anda yang lain.

5. **Apakah fitur perangkat yang tidak diperlukan telah dinonaktifkan?** Jika perangkat Anda memiliki fitur yang tidak diinginkan atau tidak diperlukan (seperti kamera atau mikrofon), fitur tersebut sebaiknya dinonaktifkan jika memungkinkan.

Berikan upaya ekstra

Cari pengaturan konfigurasi yang menyebutkan pengaktifan akses jarak jauh ke antarmuka administrasi web perangkat dari LAN lokal atau WAN/internet. Pastikan pengaturan tersebut diatur ke LAN lokal, kecuali jika Anda sendiri memerlukan akses jarak jauh.

Merawat perangkat IoT

Ada beberapa hal penting yang perlu diingat setelah perangkat IoT Anda disiapkan dan digunakan. Hal-hal tersebut meliputi:

1. **Reboot perangkat Anda secara berkala.** Virus mungkin ada jika perangkat IoT mulai menjadi lambat atau tidak dapat dioperasikan. Sebagian besar malware tersimpan di memori dan dapat dengan mudah dihapus dengan menyalakan perangkat reboot, yaitu dengan mematikan dan menghidupkannya kembali. Jika perangkat tetap lambat atau tidak dapat dioperasikan setelah dinyalakan ulang, cobalah pengaturan ulang pabrik. Namun, perlu diingat bahwa hal ini dapat menghapus semua data pengguna dan pengaturan pribadi Anda.

2. **Terapkan pembaruan rutin.** Beberapa perangkat menerapkan pembaruan secara otomatis. Bagi perangkat yang tidak menerapkan pembaruan secara otomatis, hubungi produsen secara berkala dan terapkan pembaruan saat tersedia. Ketika pembaruan tidak lagi tersedia untuk perangkat Anda, pertimbangkan untuk beralih ke perangkat yang lebih baru yang menyediakan pembaruan. Perangkat yang tidak memiliki akses ke pembaruan keamanan tidak akan terlindungi jika ditemukan kerentanan baru, dan perangkat ini dapat menjadi risiko bagi jaringan, privasi, dan data Anda.

3. **Matikan perangkat Anda saat tidak digunakan.** Membiarkan perangkat yang tidak digunakan dan tidak dipantau tetap menyala dan terhubung ke jaringan Wi-Fi Anda dalam waktu lama dapat meningkatkan kemungkinan perangkat Anda diserang. Salah satu opsi untuk mencapai hal ini secara otomatis adalah dengan menggunakan pengatur waktu stopkontak agar hanya menyediakan daya ke perangkat selama jam-jam yang ditentukan.

4. **Perhatikan peningkatan signifikan dalam penggunaan internet atau tagihan bulanan Anda.** Peningkatan signifikan dalam penggunaan internet atau tagihan dapat mengindikasikan bahwa perangkat Anda telah disusupi. Kecuali jika hal ini akan diselidiki oleh departemen TI di perusahaan Anda, pengaturan ulang pabrik harus diterapkan (namun perlu diingat bahwa ini dapat menghapus semua data pengguna dan pengaturan pribadi Anda), diikuti dengan perubahan kata sandi Anda.

Membuang satu perangkat IoT

Membuang perangkat (dengan membuang atau menjualnya) dapat memudahkan orang lain mengakses informasi atau data pribadi Anda. Cara untuk mencegah hal ini antara lain:

1. **Hapus semua data dan informasi pribadi.** Produsen harus menyediakan metode untuk menghapus data dan informasi pribadi Anda, baik dari perangkat maupun aplikasi terkait. Menghapus informasi pribadi Anda memastikan tidak ada yang mendapatkan akses setelah Anda membuang perangkat. Hapus akun online Anda jika tidak lagi diperlukan tanpa perangkat IoT.

2. **Lakukan reset pabrik pada perangkat.** Reset pabrik dirancang untuk menghapus data yang tersimpan di penyimpanan lokal dan mengatur ulang kata sandi, nama pengguna, dan pengaturan ke pengaturan asal. Periksa buku panduan pengguna perangkat atau situs web produsen untuk informasi tentang cara melakukan reset pabrik.

3. **Lepaskan perangkat dari ponsel dan perangkat lain.** Membuang perangkat yang masih memiliki akses ke perangkat lain, jaringan, atau akun online Anda berpotensi membuat orang lain mendapatkan akses. Pastikan Anda memeriksa perangkat lain dan menghapus semua pemasangan dengan perangkat yang akan Anda buang. Hapus semua izin yang diberikan ke aplikasi seluler yang tidak lagi diperlukan.

4. **Lepaskan semua media yang dapat dilepas (misalnya, flash drive USB, kartu memori, dll.) yang terpasang pada perangkat.** Media yang dapat dilepas mungkin berisi data pribadi yang tidak terhapus saat pengaturan ulang pabrik dan harus dihapus, dimusnahkan, dan dibuang secara terpisah dari perangkat.

Bantuan

Hubungi Pusat Keamanan Siber Australia di Australian Signals Directorate melalui sur-el ke asd.assist@defence.gov.au atau hubungi Hotline 24/7 untuk bantuan mendesak di **1300 CYBER1** (**1300 292 371**).

Laporkan kejahatan siber ke ReportCyber di www.cyber.gov.au/report

Hubungi IDCARE melalui situs web mereka www.idcare.org jika Anda mengalami pencurian identitas.

Kunjungi www.cyber.gov.au untuk mendapatkan saran bagi Anda dan keluarga. Daftar Layanan Peringatan ACSC gratis untuk ancaman daring terkini.

Mari jadikan Australia tempat teraman untuk terhubung daring.

Untuk nasihat keamanan siber, kunjungi www.cyber.gov.au

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.

Hak Cipta

Penggunaan lambang Coat of Arms

Persyaratan penggunaan Lambang Coat of Arms diperinci di situs web Department of the Prime Minister and Cabinet Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

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.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre