Menjaga organisasi Anda tetap aman saat online

Mengapa keamanan siber penting bagi kelompok komunitas dan organisasi?

Halaman ini berisi saran dan sejumlah langkah yang dapat Anda lakukan untuk melindungi kelompok komunitas atau organisasi Anda dari ancaman keamanan siber. Tersedia juga panduan terpisah bagi individu untuk menjaga diri mereka tetap aman saat online.

Saran ini berdasarkan ancaman yang paling umum dan serius.

- Pembaruan – pastikan perangkat lunak di semua perangkat Anda selalu diperbarui untuk menambal celah keamanan apa pun.
    - Perbarui semua perangkat milik kelompok komunitas atau organisasi Anda. Ini termasuk telepon, komputer, ruter WiFi, dan semua perangkat lainnya yang terhubung ke internet – termasuk perangkat pintar.
    - Gunakan pembaruan otomatis apabila memungkinkan.
- Autentikasi dua faktor (2FA) – memberikan keamanan tambahan pada akun Anda dengan mewajibkan kata sandi dan satu langkah tambahan, misalnya kode dari aplikasi di ponsel Anda.
    - Catatan: Keamanan ini juga disebut autentikasi multifaktor (MFA), verifikasi dua langkah (2SV) dan banyak nama lainnya.
    - Aktifkan 2FA di semua akun milik kelompok komunitas atau organisasi Anda.
    - Apabila memungkinkan, coba gunakan jenis 2FA yang tahan terhadap phishing, artinya Anda tidak dapat ditipu untuk melakukan sesuatu. Jenisnya bisa berupa kunci keamanan fisik atau sesuatu seperti sidik jari atau ID wajah.
- Pantau semua akun online Anda – pastikan mantan anggota tidak menyimpan akses akun mereka setelah keluar dari kelompok komunitas atau organisasi.
    - Jika lebih dari satu orang dapat mengakses akun yang sama, pastikan mereka memiliki login yang berbeda, dan mereka mengaktifkan 2FA.
    - Buat daftar yang berisi semua akun pengguna dan nonaktifkan akun yang tidak dibutuhkan, seperti ketika staf keluar.
    - Daftarkan semua perangkat yang diberikan kepada anggota Anda dan ingat untuk meminta agar perangkat itu dikembalikan dan melakukan reset pabrik jika orang tersebut keluar dari perusahaan. Anda mungkin juga perlu mengubah kode fisik untuk akses bangunan.
- Periksa siapa saja yang dapat mengakses akun online Anda – orang-orang di kelompok komunitas atau organisasi Anda seharusnya hanya memiliki akses ke bagian yang diperlukan.
    - Jika akun seseorang diretas, langkah ini akan membatasi kerusakan yang dapat diakibatkan peretas.
    - Periksa secara rutin dan hapus izin yang tidak diperlukan.

    - Jika Anda memiliki akun "admin" tunggal yang digunakan oleh sejumlah orang, awasi akun ini untuk mendeteksi aktivitas yang tidak lazim. Upayakan untuk membatasi akun semacam ini, terutama untuk tugas sehari-hari.
    - Aturan yang sama juga berlaku untuk akses administrator ke semua perangkat, seperti ruter.
- Tinjau kontrak Anda dengan penyedia layanan – jika Anda telah mempekerjakan seseorang untuk melakukan layanan TI.
    - Pastikan mereka memilki perlindungan keamanan siber yang diterapkan dan sesuai dengan kebutuhan kelompok komunitas atau organisasi Anda.
- Ketahui bagaimana semua akun dan sistem Anda berinteraksi – memahami semua hubungannya akan membantu Anda mengetahui di mana penyerang berpotensi akan masuk.
    - Tinjau hubungan antar sistem Anda, misalnya email, penyimpanan awan, dan platform akuntansi.
    - Pertimbangkan untuk menggunakan Virtual Private Network (VPN) untuk tambahan keamanan online. Menggunakan VPN akan menyembunyikan aktivitas online Anda dari orang-orang yang mungkin mencoba melacak Anda. Keamanan ini terutama bermanfaat jika ada anggota kelompok komunitas atau organisasi Anda yang terhubung dalam jarak jauh.
- Pastikan pegawai Anda 'pintar siber' – orang-orang di kelompok komunitas atau organsasi Anda lebih berpotensi menjadi target daripada sistem Anda.
    - Berikan pelatihan keamanan siber dasar kepada semua staf. Situs web Own Your Online Own Your Online | NCSC memiliki berbagai macam saran dan kiat untuk membantu Anda agar tetap aman saat online dan cara mengenali penipuan.
    - Ingatkan mereka bahwa hal ini penting untuk akun pribadi mereka dan juga akun yang mereka gunakan untuk organisasi Anda.
    - Kami juga memiliki panduan buat individu untuk menjaga mereka tetap aman saat online.
- Buat perencanaan jika terjadi insiden – memiliki perencanaan tanggap darurat penting agar orang-orang tidak panik ketika terjadi insiden.
    - Perencanaan tanggap darurat insiden menjelaskan siapa dan apa yang dilakukan sewaktu terjadi insiden. Templat tersedia di sini Incident Management | NCSC
    - Masukkan dalam perencanaan apa yang harus dilakukan jika ponsel, komputer, atau sistem lainnya tidak berfungsi. Perbarui perencanaan ini.
    - Simpan detail kontak setiap orang yang diperlukan dan detail cadangan seandainya cara utama untuk menghubungi mereka tidak bisa dilakukan (seperti email).
    - Simpan juga perencanan ini di suatu tempat di luar sistem Anda, untuk berjaga-jaga jika Anda tidak bisa mengaksesnya.