Modul 6 – Membangun Cyber Security Plan untuk UMKM

Panduan praktis menyusun langkah-langkah sederhana namun efektif untuk meningkatkan keamanan digital bisnis Anda — dari checklist dasar hingga rencana aksi nyata.

EDY SUSANTO - FOUNDER CSIX SECURITY

Tujuan Pembelajaran

Di akhir modul ini, Anda akan memiliki pemahaman yang jelas dan rencana yang dapat langsung diterapkan untuk melindungi bisnis Anda dari ancaman siber.

Cyber Security Checklist

Daftar periksa keamanan siber yang dirancang khusus untuk kebutuhan UMKM

Kebijakan Keamanan Dasar

Menetapkan aturan dan standar keamanan yang mudah dipahami dan diterapkan

Incident Response

Langkah tanggap darurat saat terjadi insiden keamanan di bisnis Anda

Roadmap Keamanan

Rencana bertahap untuk meningkatkan keamanan bisnis secara berkelanjutan

🎯 **Outcome:** Peserta memiliki rencana nyata dan dapat langsung diimplementasikan untuk meningkatkan keamanan bisnis mereka.

Cyber Security Checklist UMKM

Mulailah dengan mengevaluasi kondisi keamanan bisnis Anda saat ini. Checklist ini mencakup area-area paling kritis yang harus diamankan terlebih dahulu.

🔐 Akun & Kata Sandi

- [ ] Gunakan kata sandi minimal 12 karakter
- [ ] Aktifkan autentikasi dua faktor (2FA)
- [ ] Jangan gunakan kata sandi yang sama di berbagai platform
- [ ] Gunakan password manager

💻 Perangkat & Jaringan

- [ ] Update sistem operasi dan aplikasi secara rutin
- [ ] Pasang antivirus yang terpercaya
- [ ] Pisahkan WiFi operasional dan WiFi tamu
- [ ] Backup data secara berkala ke cloud dan lokal

Kebijakan Keamanan Dasar

Kebijakan keamanan tidak harus rumit. Untuk UMKM, yang terpenting adalah aturan yang sederhana, tertulis, dan benar-benar dijalankan oleh seluruh tim.

📋 Aturan Penggunaan Perangkat

Tentukan siapa yang boleh menggunakan perangkat kerja, untuk keperluan apa saja, dan larangan menginstal aplikasi tanpa izin. Pisahkan perangkat pribadi dan perangkat kerja jika memungkinkan.

🔑 Kebijakan Akses Data

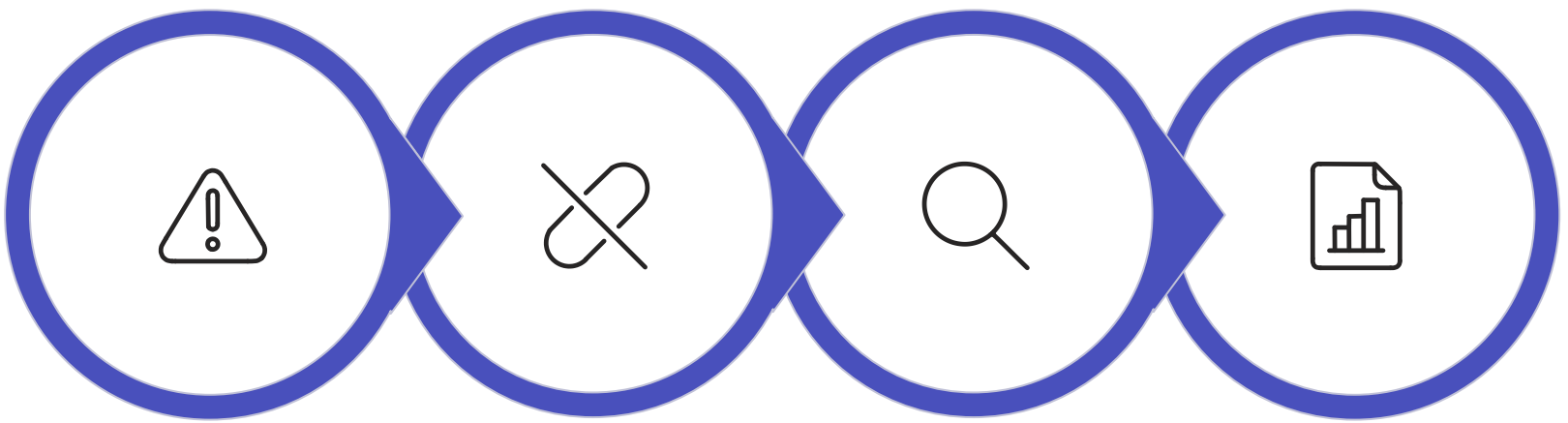
Terapkan prinsip *least privilege* — karyawan hanya boleh mengakses data yang mereka butuhkan. Buat daftar siapa yang memiliki akses ke sistem keuangan, data pelanggan, dan informasi sensitif lainnya.

📧 Aturan Komunikasi Digital

Tetapkan kebijakan penggunaan email bisnis, larangan berbagi informasi sensitif melalui WhatsApp pribadi, dan prosedur verifikasi sebelum melakukan transfer keuangan berdasarkan instruksi digital.

Incident Response Sederhana

Ketika insiden terjadi, panik adalah musuh terbesar. Dengan prosedur yang jelas dan sudah disiapkan sebelumnya, tim Anda dapat merespons dengan cepat dan terorganisir untuk meminimalkan kerugian.



Deteksi & Lapor

Isolasi

Investigasi & Pemulihan

Evaluasi

Kecepatan respons menentukan seberapa besar dampak yang ditimbulkan. Tujuan utama adalah menghentikan penyebaran, memulihkan operasional, dan mencegah kejadian serupa terulang kembali.

Siapa yang Harus Dihubungi Saat Terjadi Insiden?

Jangan mencari nomor telepon saat sedang panik. Siapkan daftar kontak darurat ini jauh sebelum insiden terjadi dan pastikan seluruh tim mengetahuinya.

BSSN (Badan Siber dan Sandi Negara)

Lembaga pemerintah resmi untuk penanganan insiden siber nasional. Hubungi melalui **pusatops.bssn.go.id** atau hotline **0800-1234-BSSN** untuk mendapatkan asistensi teknis.

Bank & Penyedia Pembayaran

Segera hubungi bank atau platform pembayaran Anda jika terjadi kebocoran data finansial atau transaksi mencurigakan. Pemblokiran cepat dapat mencegah kerugian lebih besar.

Konsultan IT / Vendor Keamanan

Miliki kontak vendor IT atau konsultan keamanan siber yang Anda percaya. Minta mereka menyediakan layanan darurat 24 jam atau setidaknya respons cepat di hari kerja.

Edukasi Karyawan dan Tim

Teknologi secanggih apapun tidak akan efektif jika tim Anda tidak memahami ancaman siber. Manusia adalah lapisan pertahanan pertama — sekaligus titik terlemah — dalam keamanan digital bisnis Anda.

Topik Pelatihan Wajib

- Mengenali email phishing dan tautan berbahaya
- Cara membuat dan mengelola kata sandi yang kuat
- Prosedur pelaporan insiden internal
- Keamanan saat bekerja dari luar kantor (remote)
- Social engineering dan manipulasi psikologis

Metode Edukasi yang Efektif

- **Pelatihan Rutin Bulanan**

  Sesi singkat 30 menit setiap bulan lebih efektif daripada pelatihan panjang setahun sekali

- **Simulasi Phishing**

  Kirim email phishing simulasi untuk mengukur kesadaran tim secara langsung

- **Poster & Reminder Digital**

  Pasang pengingat visual di area kerja dan grup komunikasi internal

Roadmap Keamanan UMKM

Keamanan siber dibangun secara bertahap. Tidak perlu sempurna dari awal — yang penting adalah konsisten bergerak maju. Berikut adalah panduan bertahap selama 12 bulan pertama.

1

Bulan 1–2: Fondasi

Audit aset digital, ganti semua kata sandi, aktifkan 2FA, dan pasang antivirus di semua perangkat

2

Bulan 3–4: Kebijakan

Buat dokumen kebijakan keamanan dasar, tentukan hak akses karyawan, dan buat prosedur backup rutin

3

Bulan 5–6: Edukasi

Lakukan pelatihan keamanan siber pertama untuk seluruh tim dan siapkan kontak darurat insiden

4

Bulan 7–12: Penguatan

Evaluasi celah keamanan, tingkatkan alat keamanan, lakukan simulasi insiden, dan perbarui kebijakan secara berkala

💡 **Tips:** Mulai dari yang paling mudah dan paling kritis terlebih dahulu. Konsistensi lebih penting daripada kesempurnaan.

Final Project: Cyber Security Action Plan

Saatnya menerapkan semua yang telah Anda pelajari! Buat **Cyber Security Action Plan** untuk bisnis Anda sendiri sebagai proyek akhir modul ini.

1

Identifikasi Aset Digital

Daftarkan semua aset digital bisnis Anda: website, akun media sosial, sistem kasir, data pelanggan, dan email bisnis. Tentukan mana yang paling kritis untuk dilindungi.

2

Penilaian Risiko

Identifikasi ancaman yang paling relevan dengan jenis bisnis Anda dan tentukan tingkat risiko (tinggi/sedang/rendah) untuk setiap aset digital yang telah didaftarkan.

3

Rencana Tindakan

Susun daftar tindakan konkret yang akan dilakukan dalam 30, 60, dan 90 hari ke depan. Cantumkan siapa yang bertanggung jawab dan kapan targetnya selesai.

4

Anggaran & Sumber Daya

Estimasikan biaya yang diperlukan untuk implementasi, termasuk alat keamanan, pelatihan, dan konsultasi jika diperlukan. Prioritaskan langkah yang gratis atau berbiaya rendah terlebih dahulu.

Rangkuman & Langkah Selanjutnya

Selamat! Anda telah menyelesaikan Modul 6. Keamanan siber bukan tujuan akhir, melainkan sebuah perjalanan berkelanjutan. Bisnis yang aman adalah bisnis yang siap tumbuh.

✅ Yang Sudah Dipelajari

- Checklist keamanan siber UMKM
- Cara membuat kebijakan keamanan
- Prosedur incident response
- Edukasi tim dan karyawan
- Roadmap keamanan 12 bulan

🚀 Tindakan Minggu Ini

- Download dan isi template Action Plan
- Audit kata sandi dan aktifkan 2FA
- Bagikan checklist ke seluruh tim
- Tentukan penanggung jawab keamanan
- Jadwalkan pelatihan pertama tim

> "Keamanan siber bukan hanya urusan IT — ini adalah urusan bisnis. Satu langkah pencegahan hari ini bisa menghemat jutaan rupiah kerugian di masa depan."

Edy Susanto - Founder CSIX Security