Mid 2020 Cyber Security Threat, Tips dan Proposal Strategi Mitigasi Nasional

Penulis:
Onno W. Purbo

EXECUTIVE SUMMARY

COVID-19 berakibat Work From Home (WFH) menjadi New Normal. Perimeter pertahanan yang selama ini cukup di lingkungan Office (Kantor) harus di perluas mencakup rumah bahkan pribadi. Seberapa serius masalah kejahatan dunia maya? Studi Cybersecurity Ventures memperkirakan kerugian dunia $ 6 triliun pada tahun 2021. Dengan konsentrasi serangan hacker setiap 39 detik, rata sekitar 2.244 kali sehari. Sialnya rata-rata waktu untuk mengidentifikasi pelanggaran adalah 206 hari (tahun 2019). Hal ini mengakibatkan siklus hidup rata-rata suatu pelanggaran (dari pelanggaran hingga penahanan) adalah 314 hari, butuh waktu hampir satu tahun untuk bisa menahan pelaku serangan siber.

Yang mengerikan, tend terbaru serangan di dominasi oleh Artificial Intelligence (AI), Machine Learning – seperti, Deep Fakes & Audio Deep Fakes - yang memungkinkan pembuatan video hoax dengan suara sangat mirip sasaran yang dapat sangat menipu kontituen pemilu, sehingga akan memusingkan para politikus, partai, pemerintah di PILPRES, PILKADA mendatang. Serangan paling mematikan masih di kuasai oleh crypto-virus terutama ransomeware, di susul oleh tipe serangan lainnya seperti Phising, Cloud Jacking, kerentanan API, Remote Worker Endpoint Security, dan Internet Of Things (IoT). Privasi data menjadi sangat strategis, serangan yang terutama ditujukan untuk memperoleh informasi identitas pribadi yang pada akhirnya dapat di jadikan uang.

Mungkinkah WFH bertahan dalam lingkungan siber yang keras? Tentunya bisa! Pengguna perlu selalu perbarui perangkat lunak, menggunakan anti-virus & firewall, menggunakan kata sandi kuat dengan tool manajemen kata sandi, menggunakan otentikasi dua faktor atau multi-faktor, mempelajari tentang teknik penipuan phishing, melindungi Informasi Identifikasi Pribadi (PII), menggunakan perangkat seluler anda dengan aman, backup data secara teratur, jangan menggunakan Wi-Fi umum, meninjau akun online & laporan kartu kredit secara teratur. Pada tingkat Enterprise / Corprate paling tidak perlu menentukan batas, menentukan lingkungan perangkat lunak, memperkuat aset jaringan, menilai kerentanan dan menerapkan Rencana remediasi, meninjau kembali hak istimewa akses administratif di seluruh perusahaan.

Pada tingkat nasional, kita dapat mengadopsi Strategi Mitigasi Siber yang berawal dari Visi, dengan mengadopsi pendekatan komprehensif dan prioritas yang disesuaikan, inklusivitas, kemakmuran ekonomi dan sosial, Hak Asasi Manusia (HAM), manajemen risiko dan ketahanan, serangkaian Instrumen kebijakan yang sesuai, kepemimpinan yang jelas, peran dan alokasi sumber daya, dan lingkungan yang Trusted. Ini merupakan sebuah siklus dengan tahapan inisiasi, Inventarisasi dan Analisis, Produksi Strategi Keamanan Siber Nasional, Implementasi. Mengembangkan rencana aksi, Pemantauan dan evaluasi.

DAFTAR ISI

TREND SERANGAN

Dalam enam bulan terakhir, cara kita hidup dan bekerja telah berubah secara drastis, sangat berbeda dengan sebelumnya. Singkat kata, kehidupan di bumi menjadi online. Perubahan itu terjadi tidak bertahap tetapi dalam waktu sekejap. Hampir semuanya berbeda sekarang, dari cara kita melakukan hubungan dengan orang, bekerja atau bahkan memesan makanan. Work From Home (WFH) menjadi new normal. Perubahan ini semua menyebabkan pergeseran drastis dunia cyber.

Ketika kita tidak sedang membicarakan atau memikirkan tentang pandemi COVID-19, maka topik hangat yang menjadi bahan diskusi adalah tentang serangan siber. Menarik untuk dicatat bahwa COVID-19 maupun serangan siber memiliki banyak kesamaan:

- Keduanya pada dasarnya adalah pandemi. Sama seperti wabah virus corona, serangan keamanan siber juga berlangsung dalam skala global dan terjadi setiap beberapa detik.
- Seperti halnya virus corona yang menyebar dari orang ke orang, malware keamanan siber juga dapat menyebar dengan cepat dari komputer ke komputer dari satu jaringan ke jaringan lain.
- Serangan dunia maya berpotensi membuat usaha kita gulung tikar, seperti yang dilakukan pandemi virus corona saat ini terhadap bisnis di mana pun.

New Normal telah menciptakan tantangan di samping peluang. Perubahan infrastruktur yang dibuat oleh perusahaan untuk memungkinkan akses jarak jauh juga membutuhkan pelaku ancaman untuk beradaptasi dengan dunia hybrid yang mengintegrasikan teknologi cloud. Selain itu, penyebaran file Virus Corona dan upaya penelitian global untuk menemukan vaksin telah menciptakan opsi phishing baru dan menjadikan lembaga penelitian medis sebagai target incaran para pelaku kriminal pada tingkat negara. Kami akan membahas efek ini dan lebih banyak fokus pada aspek lanskap ancaman, sambil memberikan contoh dan statistik peristiwa dunia nyata. Berikut beberapa tren serangan dunia maya:

Deepfakes

Deepfakes adalah kombinasi dari kata "deep learning" dan "fake". Deepfakes terjadi ketika teknologi kecerdasan buatan (Artificial Intelligence / AI) membuat gambar dan suara palsu yang tampak nyata. Deepfakes memungkinkan untuk memanipulasi gambar atau video dari seseorang untuk menggambarkan beberapa aktivitas yang sebenarnya tidak terjadi. Ada banyak spekulasi bahwa deepfakes mungkin pada akhirnya akan muncul sebagai ancaman keamanan siber utama, yang digunakan untuk maksud jahat. Teknologi audio deepfake memungkinkan kita membuat suara yang mirip dengan para politisi / selebrity. Deepfake dapat membuat video di mana kata-kata seorang politisi / selebrity / aktor dimanipulasi, membuatnya tampak bahwa pemimpin politik mengatakan sesuatu yang padahal tidak pernah mereka janji-kan, sehingga terkesan shahih padahal hoax. Untuk melakukan ini semua kita cukup menggunakan foto target sasaran, dengan 10 detik sample suara korban, sehingga sangat mengerikan terutama dengan adanya banyak PEMILU (PILPRES, PILKADA dll) tidak lama lagi. Teknik serangan ini mempunyai banyak turunan serangan yang tidak kalah canggih, seperti:

- Identitas Sintetis - Identitas sintetis adalah bentuk penipuan identitas di mana para penipu menggunakan campuran kredensial yang nyata dan palsu untuk menciptakan ilusi orang sungguhan. Misalnya, penjahat dapat membuat identitas sintetis yang menyertakan alamat fisik yang sah. Nomor KTP, KK, SIM dll dan tanggal lahir yang terkait dengan alamat itu, mungkin tidak sah.
- Serangan dunia maya yang didukung AI - Menggunakan kecerdasan buatan, peretas dapat membuat program yang meniru perilaku manusia yang diketahui. Para peretas ini kemudian

dapat menggunakan program ini untuk mengelabui orang agar memberikan informasi pribadi atau keuangan mereka.

- Serangan Hacker pada AI / machine learning – Machine Learning membutuhkan banyak data training untuk dapat mengembangkan model untuk prediksi. Tahapan ini merupakan tahapan paling rentan dalam sistem AI. Dalam serangan ini, dilakukan poisoning terhadap training data, hacker menyuntikan data buruk pada program AI sehingga AI akan salah. Contoh, beberapa hacker telah menggunakan serangan poisoning data pada sistem AI untuk menghindari pendeteksi spam.
- Disinformasi di media sosial - Anda mungkin pernah mendengar istilah "hoax". Ini juga dikenal sebagai disinformasi, penyebaran berita dan informasi yang disengaja yang tidak akurat dan dirancang untuk membujuk orang - seringkali pemilih - untuk mengambil tindakan tertentu atau memegang keyakinan tertentu. Disinformasi sosial seringkali menyebar melalui media sosial seperti Facebook dan Twitter. "Hoax" menjadi topik hangat selama dan setelah pemilihan presiden.

Ada kemungkinan teknik deepfake digunakan dalam upaya untuk memanipulasi PEMILU, PILKADA dll. Kita mungkin juga menyaksikan ancaman keamanan siber lainnya, seperti penggunaan deepfake untuk melakukan penipuan melalui identitas sintetis, dan munculnya organisasi deepfake-as-a-service. 2020 mungkin juga tahun ketika deepfakes terus melakukan penipuan phishing yang lebih meyakinkan daripada sebelumnya, yang pada akhirnya dapat merugikan dunia usaha, pemerintah dan politik dalam jumlah besar.

Serangan Phishing

Penipuan phishing biasanya menggunakan manipulasi psikologis untuk mencuri kredensial pengguna baik untuk serangan lokal maupun serangan layanan cloud. Perlu di catat bahwa hampir 78 persen insiden spionase dunia maya pada tahun 2019 terkait dengan phishing. Sialnya, jumlah ini kemungkinan meningkat pada tahun 2020, dengan upaya phishing kini diluncurkan melalui aplikasi cloud dan bukan melalui email tradisional. Kepercayaan implisit oleh pengguna cloud tempat kerja mereka akan secara tidak sengaja membuat mereka lebih rentan terhadap taktik phishing.

Advanced Ransomware dan Targeted

Serangan ransomware telah menjadi perhatian utama bisnis selama beberapa tahun terakhir. Alasan mengapa ransomware bertahan begitu lama adalah kesederhanaan relatif yang dapat digunakan penyerang untuk mencapai efek yang menghancurkan. Kit ransomware sangat murah dan tersedia di web gelap. Tahun 2020 akan melihat munculnya serangan ransomware yang sangat canggih dan tertarget. Kepala cyber investigation di McAfee, John Fokker, memprediksikan bahwa dunia bawah tanah ransomware kemungkinan besar akan berkonsolidasi, menghasilkan terciptanya keluarga malware-as-a-service yang lebih sedikit tetapi lebih kuat yang akan bekerja sama satu sama lain. Dia lebih lanjut menambahkan bahwa akan ada kelanjutan dari ransomware paling kuat yang menggunakan penggunaan struktur afiliasi untuk membuat ancaman mereka lebih serius. Ini adalah penyebab utama kekhawatiran karena efek dari satu serangan ransomware dapat sangat merusak bisnis kecil dan menengah, yang menyebabkan biaya selangit terkait dengan waktu henti dan pemulihan. Turunan Ransome yang berbahaya adalah sebagai berikut:

- Double Extortion (Pemerasan Ganda) - Aktor ransomware telah mengadopsi strategi baru; selain membuat file korban tidak dapat diakses, mereka sekarang mengekstrak data dalam jumlah besar sebelum dienkripsi pada tahap akhir serangan. Para korban yang menolak tuntutan pembayaran akan menemukan data mereka yang paling sensitif ditampilkan secara publik di Internet.

Cyber Warfare

Aktivitas dunia maya dari negara mengalami lonjakan intensitas dan peningkatan yang luar biasa. Pada saat cara tradisional untuk mengumpulkan intelijen dan pengetahuan tidak lagi memungkinkan karena adanya pembatasan jarak sosial, penggunaan senjata siber ofensif untuk mendukung misi nasional tampaknya telah meluas. Sasarannya bisa saja tentang pemahaman lebih baik tentang virus COVID-19 atau bisa saja lebih ekstrim untuk mengamankan operasi intelijen dengan negara serta industri sebagai sasarannya.

Cloud / Cloud Jacking

Industri diharuskan melakukan penyesuaian infrastruktur yang cepat untuk mengamankan produksinya saat bekerja dari jarak jauh. Dalam banyak kasus, ini tidak akan mungkin terjadi tanpa teknologi cloud. Namun, itu juga mengekspos lebih banyak aset yang salah konfigurasi atau hanya aset yang tidak dilindungi ke internet. Cloud Jacking kemungkinan akan muncul sebagai salah satu ancaman keamanan siber yang paling menonjol di tahun 2020 karena meningkatnya ketergantungan bisnis pada komputasi awan. Kesalahan konfigurasi akan mendorong sebagian besar insiden menurut Laporan Ancaman Sophos 2020. Trend Micro memprediksi bahwa serangan injeksi kode, baik secara langsung ke kode atau melalui thrid party library, akan digunakan secara mencolok terhadap platform cloud. Serangan ini - dari pembuatan skrip traffic dan SQL Injection - akan dilakukan untuk menyadap, mengontrol, dan bahkan memodifikasi file sensitif dan data yang disimpan di cloud. Sebagai alternatif, Penyerang akan memasukkan kode berbahaya ke third party library yang tanpa sengaja akan diunduh dan dijalankan oleh pengguna. Seperti dicatat dalam blog Forcepoint's 2020 Cybersecurity Predictions and Trends, model tanggung jawab bersama vendor cloud publik umum menyatakan bahwa penyedia layanan cloud bertanggung jawab untuk melindungi infrastruktur sementara pelanggan bertanggung jawab untuk melindungi data mereka, memantau akses, mengelola konfigurasi, mengamati perilaku pengguna yang anomali, memantau kerentanan sistem dan patching. Jadi, banyak tanggung jawab keamanan berada di pundak pengguna / pelanggan.

Kerentanan dan Pelanggaran Application Program Interface (API)

Studi terbaru oleh Imperva menunjukkan bahwa kesiapan keamanan antarmuka pemrograman aplikasi (API) biasanya tertinggal dari keamanan aplikasi web di sebagian besar organisasi saat ini. Selain itu, lebih dari dua pertiga organisasi siap menyediakan API untuk publik agar pengembang dan mitra eksternal dapat memanfaatkan ekosistem aplikasi dan platform perangkat lunak mereka.
Karena ketergantungan pada API meningkat, pelanggaran berbasis API akan menjadi lebih menonjol pada tahun 2020. Hal ini akan memicu dampak buruk pada aplikasi profil tinggi dalam proses keuangan, perpesanan, peer-to-peer, dan media sosial. Karena semakin banyak organisasi yang terus mengadopsi API untuk aplikasinya, keamanan API akan terlihat sebagai tautan terlemah, yang dapat menyebabkan ancaman cloud-native dan membahayakan data dan privasi pengguna.
Strategi Praktis untuk Meningkatkan Keamanan TI:

- Otomatiskan patch dan manajemen kerentanan untuk menjaga sistem tetap mutakhir dan terlindungi dari potensi ancaman dunia maya
- Backup sistem dan data aplikasi SaaS untuk memastikan pemulihan yang efisien dan cepat dari ransomware dan serangan lainnya
- Terapkan solusi AV / AM canggih yang menyediakan deteksi dan respons titik akhir (EDR) dan menjaga keamanan sistem Anda
- Pastikan bahwa laptop atau perangkat apa pun yang meninggalkan kantor memiliki rangkaian lengkap layanan keamanan, termasuk firewall lokal, perlindungan malware

tingkat lanjut, pemfilteran DNS, enkripsi disk dan otentikasi multi-faktor, di antara perlindungan lainnya.

- Miliki rencana respons insiden. Jika pelanggaran keamanan terjadi, Anda memerlukan rencana tindakan yang kuat untuk menangani pelanggaran tersebut secara efisien dan membuat perusahaan Anda bangkit kembali dengan kerusakan minimum dan secepat mungkin. Rencana tersebut harus mencakup strategi komunikasi untuk pemangku kepentingan internal dan eksternal, termasuk pelanggan, investor, dan lainnya. Semakin Anda mempersiapkan diri sebelumnya, Anda akan semakin siap untuk menghadapi krisis.

Remote Worker Endpoint Security

Remote Work yang terutama yang melakukan Work From Home (WFH) sering bekerja tanpa keamanan perimeter jaringan, sehingga kehilangan bagian penting dari pertahanan keamanan siber berlapis yang ada di Work From Office (WFO). Sialnya, perangkat smartphone tidak memperlihatkan seakan menutupi tanda-tanda adanya serangan phishing dan ancaman keamanan siber lainnya. Tidak heran, pakar keamanan di WatchGuard memperkirakan bahwa pada tahun 2020, 25 persen dari semua pelanggaran data akan melibatkan aset di luar lokasi, perangkat seluler, dan telecommuters. Varian yang cukup mengkhawatirkan adalah:

- Mobile Device Management (MDM) Attack - Penyerang mengembangkan teknik serangan baru di smartphone & seluler, mengubah dan meningkatkan teknik mereka untuk menghindari deteksi di tempat-tempat seperti PlayStore resmi. Dalam satu serangan inovatif, penyerang mengkontaminasi sistem Mobile Device Management (MDM) dari perusahaan internasional yang besar untuk mendistribusikan malware ke lebih dari 75% dari perangkat seluler yang dikelola-nya.
- Penduduk negara berkembang mungkin lebih rentan terhadap serangan dunia maya. Orang-orang di negara-negara ini sering melakukan transaksi keuangan melalui saluran telepon seluler tanpa jaminan, sehingga mereka lebih rentan terhadap serangan.
- Malware Seluler - Dengan semakin banyaknya pengguna yang secara bertahap berpindah dari sistem operasi desktop ke perangkat seluler mereka, jumlah data bisnis yang disimpan di perangkat seluler semakin besar dari hari ke hari. Malware seluler adalah perangkat lunak berbahaya yang dirancang khusus untuk menargetkan sistem operasi ponsel. Karena semakin banyak tugas kritis dan sensitif yang dilakukan pada smartphone, hanya masalah waktu sebelum malware seluler muncul sebagai salah satu masalah keamanan siber yang paling menonjol.
- Kerentanan Keamanan 5G-to-Wi-Fi - Kebutuhan perusahaan untuk menemukan cara baru untuk meningkatkan keamanan tidak pernah sebesar ini karena kesenjangan keterampilan keamanan siber dan meningkatnya kecanggihan serangan siber. Penyerang tidak diragukan lagi akan menemukan kerentanan baru dalam penyerahan 5G-ke-Wi-Fi. Dengan jaringan 5G yang berkembang pesat, operator nirkabel memberikan lebih banyak panggilan dan data ke jaringan Wi-Fi dalam upaya untuk menghemat bandwidth. Kerentanan perangkat lunak dalam proses penyerahan ini memberikan peluang bagi peretas untuk membahayakan keamanan. Dengan peluncuran 5G di area publik yang luas seperti bandara, pusat perbelanjaan, dan hotel, informasi suara dan data pengguna di perangkat berkemampuan seluler mereka dikomunikasikan melalui Wi-Fi Access Point. Sementara perangkat seluler memiliki kecerdasan bawaan untuk secara diam-diam dan otomatis beralih antara jaringan seluler dan Wi-Fi, peneliti keamanan telah mengidentifikasi sejumlah kerentanan dalam proses perpindahan ini. Sangat mungkin bahwa kerentanan keamanan 5G-to-Wi-Fi baru yang kritis akan terungkap pada tahun 2020

Internet Of Things (IoT)

Laporan Fortune Business menunjukkan bahwa pasar Internet of Things (IoT) kemungkinan akan tumbuh menjadi $ 1,1 triliun pada tahun 2026. Jelas bahwa penggunaan perangkat IoT yang meluas ini akan menandakan sejumlah besar ancaman keamanan siber yang semakin kompleks. Mungkin juga ada ancaman serius terhadap Internet of Medical Things (IoMT) yang dapat menjadi krisis kesehatan Internet yang serius. Fakta menunjukan bahwa mayoritas perangkat IoT baru masih dalam tahap awal berarti ada permukaan serangan yang jauh lebih besar bagi penjahat dunia maya untuk menargetkan kerentanan yang terkait dengan teknologi baru ini. Selain itu, sangat sulit untuk mengembangkan strategi keamanan siber untuk mengimbangi kemunculan cepat perangkat IoT baru. Contoh varian serangan IoT:

- Serangan cyber kendaraan - Semakin banyak mobil dan truk yang terhubung ke Internet, terutama untuk tracking pergerakan kendaraan, ancaman serangan siber berbasis kendaraan meningkat. Kekhawatirannya adalah penjahat dunia maya akan dapat mengakses kendaraan untuk mencuri data pribadi, melacak lokasi atau riwayat mengemudi kendaraan tersebut, atau bahkan menonaktifkan atau mengambil alih fungsi keselamatan.

Insider Threats (Ancaman Orang Dalam)

Laporan Investigasi Pelanggaran Data (DBIR) Verizon 2019 menunjukkan bahwa 34 persen pelanggaran melibatkan aktor internal. Ancaman orang dalam tidak hanya melibatkan serangan jahat, tetapi juga penggunaan sistem dan data secara sembrono oleh karyawan. Untuk melindungi dari ancaman ini, organisasi perlu mendeteksi, menyelidiki, dan merespons masalah yang dapat menjadi indikator serangan orang dalam dengan cepat dan akurat. Tool anti-virus dan anti-malware (AV / AM) umum biasanya tidak efektif melawan ancaman ini. Insider threat membutuhkan tool khusus untuk mendeteksi threat dengan memantau:

- Login tidak sah
- Aplikasi baru diinstal di komputer yang terkunci (lock)
- Pengguna yang baru-baru ini diberikan hak admin ke perangkat
- Perangkat baru di jaringan terbatas, dan banyak lagi.

Alat ini dapat menggabungkan pembelajaran mesin dan pemberian tag cerdas untuk mengidentifikasi aktivitas yang tidak wajar, perubahan yang mencurigakan, dan ancaman yang disebabkan oleh kesalahan konfigurasi sistem.

Privasi data

Perusahaan, penyedia medis, dan lembaga pemerintah menyimpan sejumlah besar data penting, mulai dari nomor pasien di Jamsostek hingga nomor rekening bank pelanggan. Privasi data mengacu pada cabang keamanan yang berfokus pada cara melindungi informasi ini dan menjauhkannya dari peretas dan penjahat dunia maya. Varian dari serangan ini:

- Serangan Jaringan Kesehatan & Rumah Sakit - Rumah sakit dan penyedia medis lainnya adalah target utama penjahat dunia maya karena penyedia medis ini memiliki akses ke informasi pribadi dan keuangan begitu banyak pasien. Pembobolan data dapat mengungkap informasi ini, yang kemudian dapat dijual oleh peretas di web gelap.
- Ada beberapa penyebab paling umum pembobolan data, yaitu, (1) password / kredensial lemah dan dicuri, (2) pintu belakang, kerentanan aplikasi, (3) perangkat lunak perusak, (4) social engineering, (5) terlalu banyak izin, (6) ancaman orang dalam, (7) kesalahan konfigurasi, dan (8) kesalahan pengguna.

STATISTIK SERANGAN

Seberapa serius masalah kejahatan dunia maya? Sebuah studi oleh Cybersecurity Ventures memperkirakan kejahatan ini akan merugikan dunia $ 6 triliun per tahun pada tahun 2021.
Ini adalah angka yang besar, tetapi tidak mengherankan bagi siapa pun yang mengikuti eksploitasi peretas dan penipu online. Kejahatan dunia maya telah menjadi berita besar, dengan data besar dan pelanggaran keamanan di perusahaan yang menjadi berita utama, dan ancaman dunia maya dari negara asing seperti China dan Rusia mengancam bisnis dan pemilu AS.

Masalah keamanan siber menjadi perjuangan sehari-hari untuk dunia usaha. Tren terbaru dan statistik keamanan siber mengungkapkan peningkatan besar dalam data yang diretas dan dibobol dari sumber yang semakin umum di tempat kerja, seperti perangkat smartphone dan IoT. Selain itu, penelitian keamanan baru-baru ini menunjukkan bahwa sebagian besar perusahaan memiliki data yang tidak terlindungi dan praktik keamanan siber yang buruk, membuat mereka rentan terhadap kehilangan data. Untuk berhasil melawan niat jahat, perusahaan wajib menjadikan kesadaran keamanan siber, pencegahan, dan praktik terbaik keamanan sebagai bagian dari budaya mereka.

Lima (5) besar statistik tentang serangan siber yang menarik untuk di simak adalah:

- Pengeluaran dunia untuk keamanan siber akan mencapai $170,4 miliar pada tahun 2022. (Gartner)
- 68% pemimpin perusahaan / bisnis merasa risiko keamanan siber mereka meningkat.
- Pembobolan data mengekspos 4,1 miliar catatan pada paruh pertama 2019. (RiskBased)
- 71% pelanggaran dimotivasi secara finansial dan 25% dimotivasi oleh spionase. (Verizon)
- 52% dari pelanggaran karena peretasan, 28% melibatkan malware dan 32-33% phishing atau manipulasi psikologis. (Verizon)

Untuk memberi gambaran yang lebih baik tentang keadaan keamanan keseluruhan saat ini, berikut adalah beberapa statistik keamanan siber yang perlu diketahui untuk tahun 2020. Mudah-mudahan, ini akan membantu menggambarkan kondisi serangan, termasuk pelanggaran data, statistik peretasan, berbagai jenis kejahatan dunia maya, statistik khusus industri, pengeluaran, biaya, dan bidang karier keamanan siber.

Fakta dan Statistik Keamanan Siber yang Berpengaruh

Disini di perlihatkan statistik yang dapat memberikan gambaran secara menyeluruh tentang bidang keamanan siber, beserta dampaknya.

- Pasar keamanan informasi dunia diperkirakan akan mencapai $ 170,4 miliar pada tahun 2022. (Gartner)
- 62% bisnis mengalami serangan phishing dan manipulasi psikologis pada tahun 2018. (Cybint Solutions)
- 68% pemimpin bisnis merasa risiko keamanan siber mereka meningkat. (Accenture)
- Rata-rata, hanya 5% folder perusahaan yang terlindungi dengan baik. (Varonis)
- Pembobolan data mengungkap 4,1 miliar catatan pada paruh pertama 2019. (Risk Base)
- 71% pelanggaran dimotivasi secara finansial dan 25% dimotivasi oleh spionase. (Verizon)
- 52% dari pelanggaran karena peretasan, 28% melibatkan malware dan 32-33% phishing atau manipulasi psikologis. (Verizon)
- Antara 1 Januari 2005 dan 18 April 2018 tercatat ada 8.854 pelanggaran. (ID Theft Resource Center)
- Sementara keseluruhan infeksi ransomware turun 52%, infeksi pada perusahaan naik 12% pada 2018. (Symantec)

- Jenis attachment email berbahaya teratas adalah .doc dan .dot yang mencapai 37%, tertinggi berikutnya adalah .exe sebesar 19,5%. (Symantec)
- Pada tahun 2020, perkiraan jumlah kata sandi yang digunakan oleh manusia dan mesin di seluruh dunia akan tumbuh menjadi 300 miliar. (Cybersecurity Media)

Statistik Peretasan dan Pelanggaran Data Terbesar

Meningkatnya jumlah pelanggaran berskala besar yang dipublikasikan dengan baik menunjukkan bahwa tidak hanya jumlah pelanggaran keamanan yang meningkat - tetapi juga semakin parah. Pembobolan data mengungkap informasi sensitif yang sering kali membuat pengguna yang terekspos pada risiko pencurian identitas, merusak reputasi perusahaan, dan hampir selalu membuat perusahaan bertanggung jawab atas pelanggaran kepatuhan. Melihat statistik pelanggaran data di bawah ini untuk membantu mengukur efek, motivasi, dan penyebab serangan yang merusak ini.

- Pelanggaran keamanan telah meningkat sebesar 11% sejak 2018 dan 67% sejak 2014. (Accenture)
- Hacker menyerang setiap 39 detik, rata-rata 2.244 kali sehari. (University of Maryland)
- Waktu rata-rata untuk mengidentifikasi pelanggaran pada 2019 adalah 206 hari. (IBM)
- Siklus hidup rata-rata suatu pelanggaran adalah 314 hari (dari pelanggaran hingga penahanan). (IBM)
- 500 juta konsumen, sejak tahun 2014, informasi mereka telah terpapar dalam pelanggaran data Marriott-Starwood yang dipublikasikan pada tahun 2018. (Marriott)
- 64% orang Amerika tidak pernah memeriksa untuk melihat apakah mereka terpengaruh oleh pelanggaran data. (Varonis)
- 56% orang Amerika tidak tahu langkah apa yang harus diambil jika terjadi pelanggaran data. (Varonis)
- Biaya rata-rata pelanggaran data adalah $ 3,92 juta pada 2019. (Security Intelligence)
- 83% beban kerja perusahaan akan berpindah ke cloud pada tahun 2020. (Forbes)
- Pada tahun 2016, 3 miliar akun Yahoo diretas dalam salah satu pelanggaran terbesar sepanjang masa. (NY Times)
- Pada 2016, Uber melaporkan bahwa peretas mencuri informasi lebih dari 57 juta penumpang dan pengemudi. (Uber)
- Uber mencoba membayar para peretas untuk menghapus data yang dicuri dari 57 juta pengguna dan menyembunyikan pelanggaran. (Bloomberg)
- Pada 2017, 412 juta akun pengguna dicuri dari situs Friendfinder. (Wall Street Journal)
- Pada 2017, 147,9 juta konsumen terkena dampak Pelanggaran Equifax. (Equifax)
- Pelanggaran Equifax merugikan perusahaan lebih dari $ 4 miliar secara total. (Time Magazine)
- Pada 2018, Under Armour melaporkan bahwa "My Fitness Pal" -nya diretas, memengaruhi 150 juta pengguna. (Under Armour)
- 18 Rusia, 19 orang Cina, 11 orang Iran dan satu orang Korea Utara terlibat dalam dakwaan atas tuduhan spionase yang sponsori-negara melawan Amerika Serikat. (Symantec)

Statistik Kejahatan Dunia Maya menurut Jenis Serangan

Sangat penting untuk memahami lanskap umum metrik seputar masalah keamanan siber, termasuk jenis serangan yang paling umum dan dari mana asalnya. Beberapa serangan paling umum ini termasuk serangan phishing, perburuan paus, manipulasi psikologis, serangan Distributed Denial of Service (DDoS), malware, dan ransomware. Ada malware dan virus baru yang ditemukan setiap hari. Varonis baru-baru ini menemukan malware cryptojacking Monero selama penyelidikan cryptojacking yang diam-diam mengganggu perusahaan selama lebih dari setahun.

- Pada DBIR 2019, 94% malware dikirim melalui email. (Verizon)

- Tingkat phishing menurun, turun dari 1 dari 2.995 email pada 2017, menjadi 1 dari 3.207 email pada 2018. (Symantec)
- 34% dari pelanggaran data melibatkan aktor internal. (Verizon)
- 51% bisnis mengalami serangan penolakan layanan pada tahun 2018. (Solusi Cybint)
- 61% organisasi pernah mengalami insiden keamanan IoT. (CSO Online)
- Skrip PowerShell berbahaya yang diblokir pada tahun 2018 pada endpoint meningkat 1.000%. (Symantec)
- 100.000 kelompok di setidaknya 150 negara dan lebih dari 400.000 mesin terinfeksi oleh virus Wannacry pada tahun 2017, dengan total biaya sekitar $ 4 miliar. (Technology Inquirer)
- Perangkat IoT mengalami rata-rata 5.200 serangan per bulan. (Symantec)
- 90% dari serangan eksekusi kode jarak jauh dikaitkan dengan cryptomining. (CSO Online)
- Biaya rata-rata serangan ransomware pada bisnis adalah $ 133.000. (SafeAtLast)
- Dalam sampel berbeda, 92% malware dikirim melalui email. (CSO Online)
- 48% lampiran email berbahaya adalah file kantor. (Symantec)
- 69% organisasi tidak percaya bahwa ancaman yang mereka lihat dapat diblokir oleh perangkat lunak anti-virus mereka. (Ponemon Institurte's Cost of Data Breach Study)
- Gandcab 5 mengharuskan korban membayar $ 2.499 untuk kunci dekripsi. (McAfee)
- 1 dari 36 perangkat seluler menginstal aplikasi berisiko tinggi. (Symantec)
- Pada tahun 2018, rata-rata 10.573 aplikasi seluler berbahaya diblokir setiap hari. (Symantec)
- 65% kelompok menggunakan spear-phishing sebagai vektor infeksi primer. (Symantec)
- Mirai Worm distributed denial of service (DDoS) tetap menjadi ancaman aktif dan, dengan 16% serangan, merupakan ancaman IoT paling umum ketiga pada tahun 2018. (Symantec)
- 1 dari 13 permintaan web mengarah ke malware. (Symantec)
- Deteksi ransomware lebih dominan di negara-negara dengan jumlah populasi terhubung internet yang lebih tinggi. Amerika Serikat menempati peringkat tertinggi dengan 18,2% dari semua serangan ransomware. (Symantec)
- Sebagian besar domain berbahaya, sekitar 60%, dikaitkan dengan spam campaigns. (Cisco)
- Sekitar 20% dari domain berbahaya masih sangat baru dan digunakan sekitar 1 minggu setelah terdaftar. (Cisco)

Statistik Kepatuhan Keamanan Siber dan Tata Kelola

Dengan ancaman baru yang muncul setiap hari, risiko tidak mengamankan file menjadi lebih berbahaya dari sebelumnya, terutama bagi perusahaan. Konsekuensi yang lebih parah ditegakkan saat undang-undang yang lebih ketat disahkan di wilayah di seluruh dunia. Beberapa hal menonjol dari beberapa tahun terakhir termasuk European Union's 2018 General Data Protection Regulation (GDPR) dan California's 2020 California Consumer Privacy Act (CCPA). Perusahaan perlu memperhatikan pelajaran dari GDPR, karena akan ada lebih banyak iterasi yang akan terjadi di seluruh dunia di tahun-tahun mendatang.
Sangat penting untuk mengatur izin dengan benar pada file dan membuang data lama. Menjaga klasifikasi dan tata kelola data tetap tinggi sangat penting untuk menjaga kepatuhan terhadap undang-undang privasi data seperti HIPAA, SOX, ISO 27001, dan lainnya.

- 69% perusahaan melihat mandat kepatuhan mendorong pengeluaran. (CSO Online)
- 53% perusahaan memiliki lebih dari 1.000 file sensitif yang terbuka untuk setiap karyawan. (Varonis)
- 22% dari semua folder tersedia untuk setiap karyawan. (Varonis)
- 88% perusahaan menghabiskan lebih dari $ 1 juta untuk mempersiapkan GDPR. (CSO Online)
- Google didenda $ 57 miliar karena pelanggaran GDPR oleh CNIL, badan perlindungan data Prancis. (TechCrunch)

- Perusahaan dilaporkan menghabiskan $ 9 miliar untuk mempersiapkan GDPR. (Forbes)
- Pada Desember 2018, hanya 50% perusahaan yang percaya bahwa mereka mematuhi GDPR. (Data Center Frontier)
- 15% perusahaan menemukan 1.000.000+ file terbuka untuk setiap karyawan. (Varonis)
- 17% dari semua file sensitif dapat diakses oleh semua karyawan. (Varonis)
- Rata-rata, setiap karyawan memiliki akses ke 17 juta file. (Varonis)
- Denda GDPR berjumlah $ 63 juta pada tahun pertama. (GDPR.eu)
- 1.000 sumber berita memblokir pembaca UE untuk menghindari aturan kepatuhan GDPR. (Nieman Lab)
- 61% perusahaan memiliki lebih dari 500 akun dengan kata sandi yang tidak kedaluwarsa. (Varonis)
- Bisnis menghabiskan rata-rata $ 1,3 juta untuk memenuhi persyaratan kepatuhan dan diharapkan untuk menambah $ 1,8 juta. (IAAP)
- Tim penasihat hukum membebani perusahaan FTSE 350 Inggris sekitar 40% dari anggaran GDPR mereka atau $ 2,4 juta. (Forbes)
- Sejak GDPR diberlakukan, 31% konsumen merasa pengalaman mereka secara keseluruhan dengan perusahaan telah meningkat. (Minggu Pemasaran)
- Pada tahun pertama GDPR, ada 144.000 keluhan yang diajukan ke berbagai lembaga penegakan GDPR dan tercatat 89.000 pelanggaran data. (EDPB)
- Equifax dinyatakan bertanggung jawab atas pelanggaran 2017 mereka dan didenda $ 425 juta oleh Federal Trade Commission (FTC) pada 2019. (FTC)

Statistik Siber Khusus Industri

Terkait keamanan siber, tidak semua industri diciptakan sama. Industri yang menyimpan informasi berharga seperti perawatan kesehatan dan keuangan biasanya menjadi target yang lebih besar bagi peretas yang ingin mencuri nomor Jaminan Sosial, catatan medis, dan data pribadi lainnya. Tapi sungguh, tidak ada yang aman karena industri berisiko rendah juga menjadi sasaran karena persepsi bahwa mereka akan menerapkan lebih sedikit tindakan pengamanan.

- 43% korban pelanggaran adalah bisnis kecil. (Verizon)
- Jasa Keuangan dan Manufaktur memiliki persentase tertinggi dari file sensitif yang terekspos sebesar 21%. (Varonis)
- Layanan keuangan memiliki rata-rata 352.771 file sensitif yang terpapar sementara Healthcare, Pharma, dan Biotech rata-rata memiliki 113.491 file - tertinggi saat membandingkan industri. (Varonis)
- 15% pelanggaran melibatkan organisasi Perawatan Kesehatan, 10% di industri Keuangan, dan 16% di Sektor Publik. (Verizon)
- Industri perbankan paling banyak menanggung biaya kejahatan dunia maya pada tahun 2018 sebesar $ 18,3 juta (Accenture)
- Organisasi yang lebih kecil (1-250 karyawan) memiliki tingkat email berbahaya yang ditargetkan tertinggi di 1 dari 323. (Symantec)
- Serangan ransomware WannaCry merugikan Layanan Kesehatan Nasional (NHS) lebih dari $ 100 juta. (Datto)
- Estimasi kerugian pada tahun 2019 untuk industri perawatan kesehatan adalah $ 25 miliar. (SafeAtLast)
- Gaya Hidup (15%), dan Hiburan (7%) adalah kategori aplikasi berbahaya yang paling sering dilihat. (Symantec)
- Supply chain attack naik 78% pada 2019. (Symantec)
- Trojan horse virus Ramnit sangat mempengaruhi sektor keuangan pada tahun 2017, menyumbang 53% serangan. (Cisco)

- Industri jasa keuangan menanggung biaya tertinggi dari kejahatan dunia maya dengan rata-rata $ 18,3 juta per perusahaan yang disurvei. (Accenture)
- Industri dengan jumlah serangan ransomware tertinggi adalah industri perawatan kesehatan. Serangan akan berlipat empat pada tahun 2020. (CSO Online)

Statistik Pengeluaran Keamanan dan Biaya

Pengeluaran rata-rata untuk kejahatan dunia maya meningkat secara dramatis, dan biaya yang terkait dengan kejahatan ini dapat melumpuhkan perusahaan yang tidak menjadikan keamanan siber sebagai bagian dari anggaran rutin mereka. Penganggaran keamanan siber terus meningkat karena semakin banyak eksekutif dan pembuat keputusan yang menyadari nilai dan pentingnya investasi keamanan siber.

- Pada tahun 2020, layanan keamanan diharapkan menyumbang 50% dari anggaran keamanan siber. (Gartner)
- Biaya rata-rata serangan malware di sebuah perusahaan adalah $ 2,6 juta. (Accenture)
- $ 3,9 juta adalah biaya rata-rata untuk pelanggaran data. (IBM)
- Layanan kesehatan memiliki biaya pelanggaran data tertinggi pada $ 429 per catatan. (IBM)
- Biaya rata-rata per rekaman yang dicuri adalah $ 150. (IBM)
- Total biaya kejahatan dunia maya untuk setiap perusahaan meningkat 12% dari $ 11,7 juta pada 2017 menjadi $ 13,0 juta pada 2018. (Accenture)
- Rata-rata pengeluaran keamanan tahunan per karyawan meningkat dua kali lipat, dari $ 584 pada tahun 2012 menjadi $ 1.178 pada tahun 2018. (Gartner)
- Biaya bisnis yang hilang rata-rata $ 1,42 juta. (IBM)
- Biaya rata-rata dalam waktu serangan malware adalah 50 hari. (Accenture)
- Komponen paling mahal dari serangan dunia maya adalah kehilangan informasi sebesar $ 5,9 juta. (Accenture)
- Biaya rata-rata per catatan yang hilang atau dicuri per individu adalah $ 141 - tetapi biaya tersebut berbeda-beda di setiap negara. Pelanggaran paling mahal terjadi di Amerika Serikat ($ 225) dan Kanada ($ 190). (Ponemon Institute’s Cost of Data Breach Study)
- Di perusahaan dengan lebih dari 50 ribu catatan yang disusupi, biaya rata-rata untuk pelanggaran data adalah $ 6,3 juta. (Ponemon Institute’s Cost of Data Breach Study)
- Termasuk perputaran pelanggan, peningkatan aktivitas akuisisi pelanggan, kehilangan reputasi dan berkurangnya niat baik, biaya bisnis yang hilang secara global adalah yang tertinggi untuk perusahaan A.S. dengan $ 4,13 juta per perusahaan. (Ponemon Institute’s Cost of Data Breach Study)
- Kerusakan yang terkait dengan kejahatan dunia maya diproyeksikan mencapai $ 6 triliun setiap tahun pada tahun 2021. (Cybersecurity Ventures)
- Biaya kerusakan ransomware akan meningkat menjadi $ 11,5 miliar pada 2019 dan bisnis akan menjadi korban serangan ransomware setiap 14 detik pada saat itu. (Cybersecurity Ventures)
- Amerika Serikat dan Timur Tengah menghabiskan paling banyak untuk respons pasca-pelanggaran data. Biaya di AS adalah $ 1,56 juta dan $ 1,43 juta di Timur Tengah. (Ponemon Institute’s 2017 Cost of Data Breach)
- 50% dari perusahaan besar (dengan lebih dari 10.000 karyawan) membelanjakan $ 1 juta atau lebih setiap tahun untuk keamanan, dengan 43% membelanjakan $ 250.000 hingga $ 999.999, dan hanya 7% yang membelanjakan di bawah $ 250.000. (Cisco)

Statistik Pekerjaan Keamanan Siber

Permintaan akan profesional keamanan siber terus meningkat seiring dengan tingkat serangan dan peningkatan anggaran keamanan siber. Ketidakseimbangan jumlah pekerja keamanan siber yang terampil serta tingginya permintaan untuk mengisi posisi keamanan siber telah menyebabkan kurangnya keterampilan keamanan siber.

- 82% pemberi kerja melaporkan kekurangan keterampilan keamanan siber. (ISSA)
- 61% perusahaan menganggap pelamar keamanan siber mereka tidak memenuhi syarat. (ISSA)
- Tingkat pengangguran keamanan siber adalah 0% dan diproyeksikan akan tetap ada hingga tahun 2021. (CSO Online)
- Diperkirakan pada tahun 2021, 100% perusahaan besar secara global akan memiliki posisi CISO. (Cybersecurity Ventures)
- Pada tahun 2021, diproyeksikan akan ada 3,5 juta pekerjaan keamanan siber yang tidak terisi secara global. (Cybersecurity Ventures)
- Posisi pekerjaan Information Security Analysts di AS diharapkan tumbuh 32% dari 2018-28. (Bureau of Labor Statistics)
- Posisi pekerjaan Computer Network Architect di AS diharapkan tumbuh 5% dari 2018-28. (Bureau of Labor Statistics)
- Posisi pekerjaan Computer Programmer di AS diperkirakan turun 7% dari 2018-28. (Bureau of Labor Statistics)
- Sejak 2016, permintaan Data Protection Officers (DPO) telah meroket dan meningkat lebih dari 700%, karena tuntutan GDPR. (Reuters)
- 500.000 Data Projection Officer dipekerjakan (IAAP)
- 66% profesional cyber security berjuang untuk menentukan jalur karier mereka. (ISSA)
- 60% profesional cyber security tidak puas dengan pekerjaan mereka saat ini. (ISSA)

TIP KEAMANAN SIBER PRIBADI

Untuk keamanan pribadi, berikut adalah tip keamanan minimal yang perlu di kerjakan.

Selalu Perbarui Perangkat Lunak Anda

Serangan ransomware adalah salah satu serangan paling mematikan baik untuk dunia usaha maupun personal. Salah satu tip keamanan dunia maya terpenting untuk mengurangi ransomware adalah melakukan patch perangkat lunak usang, baik sistem operasi, dan aplikasi. Ini membantu menghilangkan kerentanan kritis yang digunakan peretas untuk mengakses perangkat Anda. Berikut beberapa tip cepat untuk Anda mulai:

- Aktifkan pembaruan sistem otomatis untuk perangkat Anda
- Pastikan browser web desktop Anda menggunakan pembaruan keamanan otomatis
- Selalu perbarui plugin browser web Anda seperti Flash, Java, dll

Gunakan Anti-Virus Protection & Firewall

Perangkat lunak perlindungan anti-virus (AV) telah menjadi solusi paling umum untuk melawan serangan jahat. Perangkat lunak AV memblokir malware dan virus berbahaya lainnya agar tidak memasuki perangkat Anda dan membahayakan data Anda. Gunakan perangkat lunak anti-virus dari vendor tepercaya dan hanya jalankan satu alat AV di perangkat Anda.

Menggunakan firewall juga penting saat melindungi data Anda dari serangan jahat. Firewall membantu menyaring peretas, virus, dan aktivitas berbahaya lainnya yang terjadi melalui Internet dan menentukan lalu lintas apa yang diizinkan untuk memasuki perangkat Anda. Windows dan Mac OS X dilengkapi dengan firewallnya masing-masing, yang diberi nama Windows Firewall dan Mac Firewall. Router Anda juga harus memiliki firewall bawaan untuk mencegah serangan pada jaringan Anda.

Gunakan Kata Sandi Kuat & Gunakan Alat Manajemen Kata Sandi

Anda mungkin pernah mendengar bahwa sandi yang kuat sangat penting untuk keamanan online. Yang benar adalah kata sandi penting untuk mencegah peretas dari data Anda! Menurut kerangka kebijakan sandi baru National Institute of Standards and Technology (NIST) 2017, passwod yang digunakan harus mempertimbangkan:

- Menghilangkan campuran rumit huruf besar, simbol, dan angka. Sebaliknya, pilih sesuatu yang lebih ramah pengguna tetapi dengan setidaknya delapan karakter dan panjang maksimum 64 karakter.
- Jangan menggunakan sandi yang sama dua kali.
- Kata sandi harus mengandung setidaknya satu huruf kecil, satu huruf besar, satu angka, dan empat simbol tetapi tidak berikut &% # @ _.
- Pilih sesuatu yang mudah diingat dan tidak pernah meninggalkan petunjuk sandi di tempat terbuka atau membuatnya tersedia untuk umum agar peretas dapat melihatnya
- Atur ulang kata sandi anda jika anda lupa. Tapi, ubah sekali setahun.

Gunakan Otentikasi Dua Faktor atau Multi-Faktor

Otentikasi dua faktor atau multi-faktor adalah layanan yang menambahkan lapisan keamanan tambahan ke metode sandi standar identifikasi online. Tanpa otentikasi dua faktor, Anda biasanya

memasukkan nama pengguna dan kata sandi. Namun, dengan dua faktor, Anda akan diminta untuk memasukkan satu metode otentikasi tambahan seperti Kode Identifikasi Pribadi, kata sandi lain atau bahkan sidik jari. Dengan otentikasi multi-faktor, anda akan diminta untuk memasukkan lebih dari dua metode otentikasi tambahan setelah memasukkan nama pengguna dan kata sandi Anda.

Pelajari tentang Penipuan Phishing

Waspadalah terhadap email, panggilan telepon, dan brosur yang anda terima. Teknik phishing semakin berbahaya. Dalam upaya melakukan phishing, penyerang berpura-pura sebagai seseorang atau sesuatu pengirim tidak untuk mengelabui penerima agar membocorkan kredensial, mengklik link berbahaya, atau membuka lampiran yang menginfeksi sistem pengguna dengan malware, trojan, atau exploit kerentanan zero-day . Ini sering kali menyebabkan serangan ransomware. Faktanya, 90% serangan ransomware berasal dari upaya phishing.
Beberapa tip penting keamanan dunia maya yang perlu diingat tentang skema phishing meliputi:

- Intinya – Jangan KEPO! Jangan buka email dari orang yang tidak Anda kenal.
- Ketahui tautan mana yang aman dan mana yang tidak - arahkan kursor ke tautan untuk menemukan ke mana tautan itu mengarah
- Berhati-hatilah dengan email yang dikirim kepada Anda secara umum - lihat dan lihat dari mana asalnya dan apakah ada kesalahan tata bahasa
- Tautan berbahaya bisa datang dari teman yang telah terinfeksi juga. Jadi, berhati-hatilah!

Lindungi Informasi Identifikasi Pribadi (PII)

Informasi Identifikasi Pribadi (PII) adalah informasi apa pun yang dapat digunakan oleh penjahat dunia maya untuk mengidentifikasi atau menemukan seseorang. PII mencakup informasi seperti nama, alamat, nomor telepon, data lahir, Nomor Jaminan Sosial, alamat IP, detail lokasi, atau data identitas fisik atau digital lainnya. Informasi kartu kredit Anda harus dilindungi oleh perusahaan jika mereka mengikuti standar PCI DSS.

Di dunia media sosial baru yang "selalu aktif", Anda harus sangat berhati-hati tentang informasi yang Anda masukkan secara online. Disarankan agar Anda hanya menunjukkan sedikit tentang diri Anda di media sosial. Pertimbangkan untuk meninjau pengaturan privasi Anda di semua akun media sosial Anda, terutama Facebook. Menambahkan alamat rumah, tanggal lahir, atau informasi PII lainnya akan secara dramatis meningkatkan risiko pelanggaran keamanan. Peretas menggunakan informasi ini untuk keuntungan mereka!

Gunakan Perangkat Seluler Anda dengan Aman

Menurut McAfee Labs, perangkat seluler Anda sekarang menjadi target lebih dari 1,5 juta insiden baru perangkat lunak perusak seluler. Berikut beberapa tip cepat untuk keamanan perangkat seluler:

- Buat Kode Sandi Seluler yang Sulit - Bukan Tanggal Lahir atau PIN Bank Anda
- Instal Aplikasi dari Sumber Tepercaya
- Jaga Perangkat Anda Diperbarui - Peretas Menggunakan Kerentanan dalam Sistem Operasi Lama yang Tidak Tertandingi
- Hindari mengirimkan PII atau informasi sensitif melalui pesan teks atau email
- Manfaatkan Find my iPhone atau Android Device Manager untuk mencegah kehilangan atau pencurian
- Lakukan backup ponsel biasa menggunakan iCloud atau Mengaktifkan Backup & Sync dari Android

Backup Data Secara Teratur

Membackup data secara teratur adalah langkah yang sering diabaikan dalam keamanan online pribadi. Manajer TI dan keamanan teratas mengikuti aturan sederhana yang disebut aturan cadangan 3-2-1. Pada dasarnya, anda sebaiknyamenyimpan tiga salinan data anda di dua jenis media yang berbeda (hard drive lokal dan eksternal) dan satu salinan di lokasi di luar situs (penyimpanan cloud).

Jika anda menjadi korban ransomware atau malware, satu-satunya cara untuk memulihkan data anda adalah dengan menghapus sistem Anda dan memulihkan dari backup terakhir.

Jangan Gunakan Wi-Fi Umum

Jangan menggunakan Wi-Fi publik tanpa menggunakan Jaringan Pribadi Maya (VPN). Dengan menggunakan VPN, lalu lintas antara perangkat Anda dan server VPN dienkripsi. Ini berarti jauh lebih sulit bagi penjahat dunia maya untuk mendapatkan akses ke data Anda di perangkat Anda. Gunakan jaringan seluler Anda jika Anda tidak memiliki VPN saat keamanan penting.

Tinjau Akun Online & Laporan Kartu Kredit Anda Secara Teratur untuk Perubahan

Dengan pelanggaran Equifax baru-baru ini, semakin penting bagi konsumen untuk melindungi akun online mereka dan memantau laporan kartu kredit mereka. Pembekuan kartu kredit adalah cara paling efektif bagi anda untuk melindungi informasi kredit pribadi dari penjahat siber. Pada dasarnya, ini memungkinkan anda untuk mengunci kartu kredit Anda dan menggunakan nomor identifikasi pribadi (PIN) yang hanya anda yang akan tahu. Anda kemudian dapat menggunakan PIN ini ketika Anda perlu mengajukan kredit.

Penyebab Teratas Pelanggaran Keamanan

Insiden peretasan, phishing, dan perangkat lunak perusak menjadi penyebab nomor satu pelanggaran keamanan saat ini. Namun, yang lebih meresahkan, upaya peretasan ini adalah hasil dari kesalahan manusia dalam beberapa hal. Pendidikan dan kesadaran sangat penting dalam memerangi aktivitas kejahatan dunia maya dan mencegah pelanggaran keamanan.

TIP KEAMANAN SIBER ENTERPRISE

Di seluruh sektor komersial, industri, perawatan kesehatan, pendidikan dan pemerintah, keamanan siber menjadi perhatian utama di antara para pimpinan. Karena adanya kerentanan keamanan siber, banyak usaha telah menjadi sasaran peretas atau menjadi sasaran pelanggaran data.
Banyak hal yang dipertaruhkan dalam hal keamanan, keuangan, dan reputasi, oleh karena itu sangat penting untuk memiliki program keamanan siber enterprise / perusahaan untuk melindungi data penting.

Apa Perbedaan Cybersecurity Perusahaan dengan Cybersecurity Tradisional?

Jika kita tanyakan pada profesional IT tentang perbedaan antara keamanan siber perusahaan dari keamanan siber tradisional, maka anda dijamin memperoleh jawaban yang menggambarkan tingkat kompleksitas solusi TI di seluruh perusahaan. Walaupun yang tampak secara kasat mata, sehari-hari hanya dengan membangun firewall di sekitar perangkat keras TI di lokasi anda dan mengatakan bahwa anda telah mendapatkan keamanan siber dengan baik dibelakangnya.

Memang, serangan siber saat ini sebagian besar masih datang dari luar perusahaan. Namun demikian, 25 persen pelanggaran saat ini disebabkan oleh karyawan yang ceroboh atau, lebih buruk lagi, orang dalam yang berniat jahat. Selain itu, sebagian besar perusahaan sekarang memiliki infrastruktur TI yang merupakan perpaduan kompleks dari sistem lama, aplikasi baru, dan solusi berbasis cloud publik atau pribadi.

Apakah Keamanan Siber Perusahaan?

Keamanan siber perusahaan adalah solusi yang lebih kompleks yang mengambil premis keamanan siber lama dan memperluasnya ke semua tingkat komputasi bisnis modern. Sementara metode keamanan siber lama disusun untuk melindungi data di front lokal, strategi keamanan siber perusahaan dirancang untuk melindungi data saat berpindah antara perangkat nirkabel yang jauh dan ke server cloud.

Artinya, keamanan siber perusahaan melibatkan perlindungan infrastruktur di lokasi dan berbasis cloud perusahaan Anda serta memeriksa penyedia pihak ketiga dan mengamankan semakin banyak titik akhir yang terhubung ke jaringan anda melalui Internet of Things (IoT).

Mengapa Keamanan Siber Perusahaan Begitu Penting?

Sederhananya, data adalah mata uang masa depan. Dunia usaha membutuhkannya untuk berinteraksi dengan pelanggan dan untuk mengotomatiskan proses internal. Namun penjahat dunia maya memahami dengan tepat betapa berharganya data - itulah sebabnya segala sesuatu mulai dari ransomware hingga phishing terus meningkat. Itu juga mengapa anda ingin tetap waspada dalam melatih karyawan tentang cara menghindari kesalahan paling umum yang dapat menyebabkan masalah keamanan siber.

Ketika pelanggaran keamanan siber terjadi, akibat dari insiden ini dapat merugikan dunia usaha dan merugikan. Namun, seperti yang telah kita lihat, tidak ada lagi batas yang mudah ditentukan untuk dilindungi. Gabungkan semua ini, dan kebutuhan akan keamanan siber perusahaan yang kuat tumbuh seiring dengan inovasi teknis yang memungkinkan bisnis tumbuh dan menjadi lebih mobile serta beragam lokasi.

Cek List Keamanan Keamanan Siber Perusahaan

Untuk memulai program keamanan siber perusahaan, ada lima (5) cek list yang harus diselesaikan perusahaan anda sesegera mungkin. Setiap cek list dirancang untuk membuat organisasi anda aman namun siap menghadapi tantangan terhadap keamanan siber.

Tentukan Batasan

Untuk memastikan keamanan siber organisasi anda, anda harus memiliki serangkaian batasan di tingkat lokal dan virtual. Dalam infrastruktur komputasi anda, batas berfungsi sebagai perisai pelindung di sekitar aset informasi, seperti data rentan yang akan Anda simpan di hard drive lokal atau server cloud.

Batasan telah menjadi masalah yang semakin penting sejak munculnya dan penyebaran komputasi awan dan IoT. Sebelum awan datang, batas-batas ditetapkan di tingkat lokal. Dalam hal perlindungan aset informasi, Anda akan mempekerjakan staf TI untuk mengawasi penyimpanan, pencadangan, dan transfer data berharga.

Saat ini, Anda juga harus memiliki batasan untuk melindungi informasi saat diteruskan dari sistem lokal Anda ke server cloud pihak ketiga. Batas harus ditetapkan untuk setiap jenis data yang dapat ditransfer dari semua titik transfer yang memungkinkan. Misalnya, jika Anda memiliki tim karyawan yang terhubung di sistem komputasi perusahaan Anda dari lokasi yang berbeda, perangkat yang mereka gunakan untuk mengunduh, membuka, mengedit, mentransfer, dan mengunggah data perusahaan pribadi harus dilindungi dari semua kemungkinan metode intersepsi.

Tentukan Lingkungan Perangkat Lunak

Komponen kedua dari keamanan informasi perusahaan yang sejalan dengan definisi batasan adalah definisi lingkungan perangkat lunak perusahaan. Pada dasarnya, anda harus menentukan tujuan dan kebijakan terkait setiap jenis perangkat lunak yang digunakan dalam sistem komputer perusahaan. Jika aplikasi perangkat lunak sudah usang atau tidak memiliki tujuan apa pun dalam kerangka kerja komputasi perusahaan Anda, aplikasi tersebut harus dihapus dari sistem.

Jika organisasi anda memiliki tenaga kerja yang besar, pasti ada lusinan, bahkan ratusan karyawan dengan berbagai tingkat akses ke sistem komputer perusahaan. Jika orang terhubung dari berbagai alat tulis dan perangkat komputasi seluler, perangkat yang sama ini mungkin juga berisi program yang dapat menimbulkan ancaman terhadap lingkungan perangkat lunak perusahaan anda melalui skrip dan virus yang otomatis. Saat anda menentukan lingkungan, anda menentukan jenis perangkat lunak yang dapat dan tidak dapat bersentuhan dengan jaringan perusahaan anda.

Untuk memelihara lingkungan perangkat lunak anda dengan baik, selalu instal pembaruan dan patch terbaru dan perangkat anda harus di-scan secara teratur untuk menemukan virus. Adakan sesi pelatihan di antara staf untuk memastikan bahwa setiap orang mengetahui program dan protokol terbaru.

Perkuat Aset Jaringan

Setelah anda menentukan batasan dan lingkungan perangkat lunak jaringan komputasi, langkah selanjutnya adalah memperkuat aset dalam jaringan. Ini berarti bahwa setiap perangkat keras atau program perangkat lunak yang secara fisik atau jarak jauh terhubung ke sistem anda harus ditutup dari kemungkinan gangguan, kebocoran data atau akses tidak sah.
Untuk memperkuat aset komputasi anda, setiap komponen dalam sistem harus diperiksa dan diuji kekuatan dan kerentanannya. Jika pihak ketiga dapat membahayakan perangkat tertentu, perangkat tersebut perlu diprogram ulang atau dihapus dari sistem. Demikian juga, jika program perangkat

lunak protokol cloud dapat mengekspos data pribadi ke pencuri dunia maya, masalah ini harus diperbaiki sesegera mungkin.

Meskipun sangat penting untuk membuat jaringan anda seaman mungkin, anda juga ingin memastikan bahwa komponen sistem anda masih dapat berfungsi sesuai kebutuhan untuk operasi perusahaan anda. Dalam beberapa kasus, perusahaan akan membatasi perangkat keras dan perangkat lunak mereka untuk keamanan maksimum tetapi sebagai akibatnya memiliki masalah konektivitas.

Menilai Kerentanan dan Menerapkan Rencana Remediasi

Bahkan di jaringan yang paling kuat dan mutakhir, keamanan titik akhir terkadang dapat dikompromikan oleh kerentanan dalam aplikasi perangkat lunak. Hal ini sebagian besar disebabkan oleh kegigihan attacker dunia maya, yang terus mencari cara untuk menemukan celah dalam pembaruan program dan patch keamanan terbaru. Oleh karena itu, sangat penting untuk mengalahkan attacker dunia maya ini dalam permainan mereka dan selalu berada beberapa langkah di depan.

Untuk meminimalkan potensi kerentanan dalam sistem anda, anda harus memiliki rencana pengelolaan dan perbaikan yang dapat diterapkan dalam waktu singkat. Saat risiko keamanan atau lubang sistem ditemukan dalam jaringan komputasi perusahaan anda, tim anda harus bersiap untuk menambal secepat mungkin.

Salah satu aspek yang paling mengganggu dari pelanggaran data adalah lamanya waktu yang biasanya dibutuhkan organisasi yang terekspos untuk menemukan masalahnya. Data sensitif perusahaan dapat terbuka untuk peretas selama enam bulan atau lebih sebelum masalah ditemukan, menyebabkan kerusakan yang tak terukur pada keuangan dan reputasi perusahaan. Dengan rencana perbaikan yang efektif, tim anda harus dapat mempersingkat durasi antara penemuan dan koreksi pelanggaran sistem.

Tinjau Hak Istimewa Akses Administratif di Seluruh Perusahaan

Langkah terakhir untuk diterapkan sebagai bagian dari strategi keamanan siber perusahaan anda adalah menutup akses administratif ke semua kecuali fungsi paling vital dari personel yang berwenang. Dalam sistem komputasi perusahaan, akses administratif adalah pintu masuk yang paling dicari oleh attacker dunia maya. Oleh karena itu, penting untuk meninjau hak akses administratif saat ini di antara staf anda dan menentukan individu mana yang sebenarnya harus memiliki jenis akses ini.

Lakukan inventarisasi individu di antara staf anda yang akunnya telah diberikan hak administratif. Apakah masing-masing individu ini memainkan peran penting dalam tugas administratif perusahaan Anda? Jika ada individu yang tidak mendapatkan akses administratif, batasi hak istimewa orang tersebut. Bagi mereka yang tetap memiliki hak istimewa, akses administratif hanya boleh diberikan ketika tugas administratif penting harus dilakukan. Jika tidak, tidak seorang pun boleh masuk ke portal administratif mana pun.

Untuk implementasi lebih lanjut, sebaiknya menggunakan tenaga keamanan jaringan profesional. Atau membaca kuliah ilmu cyber security (FREE) di lms.onnocenter.or.id/moodle/

PROPOSAL STRATEGI MITIGASI NASIONAL

Dalam mengembangkan Strategi Mitigasi / Keamanan Siber Nasional, ada baiknya kita mengembangkan visi, strategi hingga langkah taktis yang mungkin di adopsi. Adopsi dan penyesuaian dengan kondisi Indonesia dari referensi yang ada di luar sana.

Proposed Visi

Visi berikut dibuat dengan membayangkan ini dilakukan oleh negara, tapi tidak terlalu bermimpi dan dapat cukup realitis untuk kondisi Indonesia. Visi dibuat lebih besar dari sekedar lingkup keamanan Siber, tapi lebih kepada lingkup negara / bangsa. Visi di tuangkan dalam empat pilah utama, sebagai berikut.

- **Pilar I: Lindungi Rakyat, Tanah Air, dan Cara Hidup.** Mengbangun mengimplementasikan jaringan dan informasi yang aman. Memastikan infrastruktur kritis di Republik ini aman. Memerangi kejahatan dunia maya dan meningkatkan / memperbaiki proses pelaporan insiden.

- **Pilar II: Promosikan Kesejahteraan.** Memberdayakan Ekonomi Digital yang Hidup dan Tangguh. Memberdayakan dan melindungi kepandaian / kemampuan bangsa Indonesia. Menngembangkan tenaga kerja keamanan siber yang unggul.

- **Pilar III: Pertahankan Kedamaian melalui Kekuatan.** Meningkatkan stabilitas dunia siber melalui norma & hukum negara yang bertanggung jawab. Mencegah perilaku dan atribut yang tidak dapat di terima di dunia maya.

- **Pilar IV: Tingkatkan Pengaruh Indonesia.** Mempromosikan Internet yang Terbuka, dapat dioperasikan, Andal, dan Aman. Membantu membangun kapasitas siber internasional.

Dalam visi ini ada beberapa prinsip dasar yang perlu di anut, adapun prinsip tersebut adalah sebagai berikut:

- Visi
- Pendekatan komprehensif dan prioritas yang disesuaikan
- Inklusivitas
- Kemakmuran ekonomi dan sosial
- Hak Asasi Manusia (HAM).
- Manajemen risiko dan ketahanan
- Serangkaian Instrumen kebijakan yang sesuai
- Kepemimpinan yang jelas, peran dan alokasi sumber daya
- Lingkungan yang Trusted

Siklus / Tahapan Strategi Mitigasi Siber Nasional

Dalam implementasi strategi mitigasi / keamanan siber nasional, tentunya tidak bisa dilakukan secara instan. Semua akan bertahap dan biasanya melalui sebuah siklus proses yang terus berulang semakin hari semakin baik.

- **Tahap I: Inisiasi.** Mengidentifikasi otoritas utama di ranah keamanan siber nasional. Membentuk komite pengarah. Mengidentifikasi pemangku kepentingan untuk dilibatkan dalam pengembangan Strategi. Merencanakan pengembangan Strategi

- **Tahap II: Inventarisasi dan Analisis.** Menilai lanskap keamanan siber nasional. Dan yang tidak kalah penting adalah menilai lanskap risiko dunia maya

- **Tahap III: Produksi Strategi Keamanan Siber Nasional.** Mendraf Strategi Keamanan Siber Nasional. Berkonsultasi dengan berbagai pemangku kepentingan. Mencari kesepakatan dan persetujuan yang bersifat formal. Menerbitkan Strategi Keamanan Siber Nasional.

- **Tahap IV: Implementasi.** Mengembangkan rencana aksi. Menentukan inisiatif yang akan dilaksanakan. Mengalokasikan sumber daya manusia dan keuangan untuk implementasi. Mengatur kerangka waktu dan metrik

- **Tahap V: Pemantauan dan evaluasi.** Membangun proses formal. Memantau kemajuan implementasi Strategi. Mengevaluasi hasil dari Strategi.

Contoh Baik Strategi Mitigasi Siber Nasional

Ada beberapa fokus yang spesifik dan baik untuk di perhatikan. Fokus ini sebetulnya saling terkait yang pada akhirnya saling terkait untuk membentuk strategi siber nasional yang kohesif.

- **Fokus 1 - Tata Kelola.** Memastikan untuk memperoleh dukungan dari tingkat manajemen tertinggi. Membentuk otoritas keamanan siber yang kompeten. Memastikan kerjasama intra-pemerintah. Memastikan kerjasama antar sektor, menghilangkan barier antar sektor. Mengalokasikan anggaran dan sumber daya khusus. Dan yang tidak kalau penting adalah mengembangkan rencana implementasi

- **Fokus 2 - Manajemen risiko dalam keamanan siber nasional.** Mendefinisikan pendekatan manajemen risiko. Identifikasi metodologi umum untuk mengelola risiko keamanan siber. Mengembangkan profil risiko keamanan siber sektoral. Menetapkan kebijakan keamanan siber

- **Fokus 3 - Kesiapsiagaan dan ketahanan.** Membangun kemampuan respons insiden siber. Menetapkan rencana darurat untuk manajemen krisis keamanan siber. Mempromosikan berbagi informasi. Melakukan latihan keamanan siber.

- **Fokus 4 - Layanan infrastruktur penting dan layanan penting.** Menetapkan pendekatan manajemen risiko untuk melindungi infrastruktur dan layanan kritis. Mengadopsi model tata kelola dengan tanggung jawab yang jelas. Tentukan baseline keamanan siber minimum. Memanfaatkan berbagai pengungkit pasar. Membangun kemitraan publik swasta

- **Fokus 5 - Pengembangan kemampuan dan kapasitas serta peningkatan kesadaran.** Mengembangkan kurikulum keamanan siber. Mendorong pengembangan keterampilan dan pelatihan tenaga kerja. Menerapkan program peningkatan kesadaran keamanan siber yang terkoordinasi. Mendorong inovasi keamanan siber dan R&D

- **Fokus 6 - Legislasi dan Regulasi.** Menetapkan legislasi kejahatan dunia maya. Mengakui dan melindungi hak dan kebebasan individu. Membuat mekanisme kepatuhan. Mendorong

pembangunan kapasitas untuk penegakan hukum. Menetapkan proses antar-organisasi. Mendukung kerja sama internasional untuk memerangi kejahatan dunia maya

- **Fokus 7 - Kerja sama internasional.** Mengakui pentingnya keamanan siber sebagai prioritas kebijakan luar negeri. Terlibat dalam berbagai ajang, inisiatif dan diskusi internasional. Mendorong kerjasama formal dan informal di dunia maya. Menyelaraskan upaya keamanan siber domestik dan internasional

REFERENSI

- - 2020, Cybersecurity for Indonesia: what needs to be done?, accessed 9 September 2020, <https://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009>
- Charles A. Sennewald and Curtis Baillie (2020). *Effective Security Management.* Seventh Edition. Butterworth-Heinemann an imprint of Elsevier.
- Check Point Research 2020, *Cyber Attack Trends: 2020 Mid-Year Repport*, accessed 9 September 2020, <https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/>
- Chiper Team 2020, 10 Personal Cyber Security Tips — #CyberAware, accessed 9 September 2020, accessed 9 September 2020, <https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>
- Chuck Easttom (2020). *Computer Security Fundamentals.* Fourth Edition. Pearson.
- Consolidated Technologies, Inc. 2020, Enterprise Cybersecurity, accessed 9 September 2020, <https://consoltech.com/blog/enterprise-cybersecurity/>
- Cyber Observer 2020, *29 Must-know Cybersecurity Statistics for 2020*, accessed 9 September 2020, <https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/>
- Cybersecurity Ventures 2020, Cybercrime Damages $6 Trillion By 2021, accessed 6 September 2020, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- Dan Rafter for NortonLifeLock 2020, *Cyberthreat trends: 15 cybersecurity threats for 2020*, accessed 9 September 2020, <https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html>
- Gupta (2020). *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*. (Brij B. Gupta · Gregorio Martinez Perez Dharma P. Agrawal · Deepak Gupta Eds). Springer.
- International Telecommunication Union 2018, Guide to Developing A National Cybersecurity Strategy, accessed 9 September 2020, <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf>
- Jann Chambers 2020, *55 Astounding Cybersecurity Statistics in 2020*, accessed 9 September 2020, <https://www.ukwebhostreview.com/blog/cybersecurity-statistics/>
- Jeff Melnick 2020, *Top 10 Most Common Types of Cyber Attacks*, accessed 9 September 2020, <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>
- John Emmitt 2020, *Top 10 Cybersecurity Threats in 2020*, accessed 9 September 2020, <https://www.kaseya.com/blog/2020/04/15/top-10-cybersecurity-threats-in-2020/>
- Joseph Migga Kizza (2020). *Guide to Computer Network Security.* Fifth Edition. Springer.
- Onno W. Purbo, e-Learning Kuliah Cyber Security, accessed 9 September 2020, <https://lms.onnocenter.or.id/moodle/course/view.php?id=115>
- Preston de Guise (2020). *Data Protection: Ensuring Data Availability.* second edition. CRC Press.
- Rob Sobers 2020, *110 Must-Know Cybersecurity Statistics for 2020*, accessed 9 September 2020, <https://www.varonis.com/blog/cybersecurity-statistics/>
- Resilience and CIIP Program at ENISA, National Cyber Security Strategies, accessed 9 September 2020, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- Tim Rains (2020). *Cybersecurity Threats, Malware Trends, and Strategies: Mitigate exploits, malware, phishing, and other social engineering attacks.* Packt>