Monthly Newsletter

September 2022

XAPIENS

Cyber Security Culture

Menyikapi dan Melindungi diri dari Tren dan Bahaya Cyber Threat

Semakin pesatnya perkembangan teknologi, maka semakin membuka peluang munculnya *cyber threat* yang dilakukan oleh pihak-pihak tidak bertanggung jawab salah satunya untuk mencuri data kita. Bahkan isu *cyber threat* seperti hacking menjadi topik cukup hangat belakangan ini, seperti kasus Bjorka dan Desorden yang sempat menghebohkan Indonesia beberapa waktu lalu. Ini kemudian menjadi semakin menyadarkan kita betapa pentingnya *cyber security awareness* serta pentingnya menjaga data dan sistem yang dimiliki agar tidak dibobol / di-*override* oleh pihak asing.

Di kesempatan kali ini, kami berdiskusi bersama dengan Cyber Security Expert Xapiens untuk mengetahui pandangan dan perspektif mereka terkait dengan *cyber threat* di luar sana seperti Bjorka, Desorden serta bagaimana upaya yang dapat dilakukan dalam rangka mengamankan dan melindungi diri dari bahaya *cyber threat* seperti hacking

Melihat hangatnya topik cyber threat belakangan ini, dari perspektif rekan-rekan, sebenarnya jenis cyber threat apa yang sedang banyak menjadi isu sekarang ini?

Sebenarnya banyak studi yang membahas akan hal ini, kebetulan di Indonesia yang sedang heboh adalah data leak atau kebocoran data. Cuma, *threat*-nya sendiri bisa bermacam-macam, dimana data leak itu sebenarnya adalah *impact*. Yang sekarang terjadi mereka melakukan serangan untuk mengambil akses ke suatu server untuk dimanfaatkan mereka sendiri, seperti salah satunya pencurian data. Nah pencurian data ini menjadi tren lagi sekarang ini.

Pernah ada studi dari Verizon di tahun lalu membahas *threat* yang paling tinggi adalah kasus *phishing attack*. Tapi memang di Indonesia kebetulan yang paling heboh *data leak* ini. Jadi kalau bicara *threat* bisa dari macam-macam, bisa dari malware yang terus berkembang, phishing yang tertinggi, atau bisa dari *system vulnerabilities*, yang mana sistem memang rentan.

Phishing mungkin di Indonesia tidak seramai ransomware, padahal phishing menjadi nomor satu. Karena phishing itu *hidden attack*, dia tidak kelihatan. Orang terjebak *phishing* kecenderungannya mereka tidak tahu terkena *phishing* atau nggak kecuali datanya sudah *breach*, beda dengan *ransomware* yang langsung muncul.

Kalau data leak sendiri, hacking menjadi istilah sering dibicarakan. Apa yang dimaksud dengan hacking? dan apa yang membuat hacking ini berbeda dari tipe serangan yang lain?

Ini dari kata "hack" yang kalau diterjermahkan membobol. Jadi melakukan *compromising* terhadap suatu sistem, itulah yang dinamakan hacking. Apabila ada yang mengatakan hacker sebagai orang yang membangunsesuatu, nah itu tidak sesuai, tidak relevan.

Jadi hacking adalah aktifitas menjebol atau menerobos suatu sistem ataupun program. Dimana hacker menyerang, menjebol, dan melakukan eksploitasi dari sistem atau aplikasi. Cara hacking sendiri bermacam-macam, seperti phishing juga sebenarnya termasuk cara / teknik melakukan hacking, kemudian ada malware, social engineering.

Kemudian kalau dari perkembangan kasus hacking ini seperti apa rekan-rekan? Dan seberapa pesat perkembangannya?

Sebenarnya kalau kasus sudah ada dan sudah ramai dari jaman dulu, kalau global dari US dan Rusia kemudian berkembang lagi di India. Dari jaman dulu sudah ramai, tapi dulu cyber crime dulu yang muncul, baru kemudian muncul hacking. Hacking di Indonesia ini kebanyakan mengadopsi dari luar, perkembangannya di negara ini sebenarnya sangat jauh apabila dibandingkan dengan global. *Cyber trend* di Indonesia sebenarnya menurun tapi memang baru-baru ini mulai meningkat lagi.

Tapi kami biasa lebih suka berbicara mengenai perkembangan *cyber security-nya*, karena sebenarnya namanya hitam, selalu ada putih. Banyak referensi yang memberitahu serangan hacking bahkan pertama kali udah di abad 17-18 pada jaman semaphore dan telegram, telekomunikasi pertama di dunia yang dibangun di prancis. Dimana pertama kali towernya disadap, informasi dicuri, dan diambil keuntungannya. Nah, bisa jadi lebih awal lagi ada kasus seperti ini.

Semakin kesini hacking semakin berkembang, seiring dengan perkembangan teknologi. Artinya ketika suatu ada teknologi baru dibangun, ada cara untuk membobolnya dan trennya sendiri juga akan semakin berkembang. Di tambah lagi *cyber security* bukan melulu soal hacking, tapi juga belajar enskripsi, pertahanan, membangun *firewall*. Seperti misalnya phishing, dulu mana ada phishing. Phishing muncul ketika email sudah menjadi media komunikasi.

Kalau cyber security merupakan divisi yang tahan dengan gejolak perubahan ekonomi. Disaat covid divisi lain mengalami penurunan, justru permintaan meningkat. Akan tetapi naiknya trend kasus saat ini seperti kebocoran data, serangan pihak luar, dan lain-lain juga menghadirkan tantangan baru dan beragam bagi para *expert* dan *cyber security engineer* untuk ditangani.

Q&A *Kalau berdasarkan dari pengalaman rekan-rekan, seberapa besar impact / pengaruhnya bagi bisnis dan perusahaan?*

Kalau dampak tergantung seberapa penting data tersebut untuk perusahaan. Ada yang kalau kena hack, mereka lebih santai karena mau mati atau hilang sekalipun datanya, karena datanya memang sama

Pertama dampaknya untuk bisnis, misalnya ketika core bisnis ada aplikasinya seperti itu kemudian aplikasinya dan databasenya kena hack, nah itu dampaknya besar sekali. Secara finansial juga, kalau ada pencurian uang apalagi kalau ada transaksi di aplikasi tersebut. Kemudian secara reputasi, trust/kepercayaan pelanggan kepada perusahaan juga pasti turun, bayangkan *customer* apakah ada yang mau kesana kalau mereka tahu data bisa tercuri, uang bisa tercuri karena

Dampak sangat signifikan apabila data dan aplikasi itu merupakan *core* bisnis mereka dan rahasia, terutama yang dilindungi undang-undang. Nah, yang paling ditakutkan oleh perusahaan adalah yang *reputational loss*, itu yang tertinggi pengaruhnya untuk mereka. Selain itu waktu dan cost juga dapat menjadi imbasnya.

Q&A *Kemudian, apa yang perlu diperhatikan bagi bisnis agar bisa melindungi diri dari kasus hacking ataupun cyber threat seperti ini?*

Yang perlu diperhatikan adalah keamanan keseluruhan, komponen apa saja yang membentuk sistem tersebut, misalnya infrastrukturnya seperti network, database, software, aplikasi. Jadi secara keseluruhan harus benar-benar diamankan, haru diuji, harus ada pemantauan, peningkatan yang dilakukan terus menerus. Selain infrastruktur juga faktor manusia. Ini juga sangat berpengaruh, anggaplah seorang admin yang memegang akses itu, seharusnya rahasia karena mereka bisa menjadi objek serangan hacker. Ketika hacker gagal menembus infrastruktur, nah mereka akan mencoba menyerang sisi manusia.

Jadi kalau kita coba lihat dari sisi 5W 1H seperti itu, pertama dari What, kita mengenal ada Namanya security object yaitu *people, process, dan technology*. Dari sisi orangnya harus *di-improve*, kemudian proses atau kebijakan gimana supaya sistem dapat berjalan dengan aman seperti misalnya dokumen *finance* hanya boleh diakses *finance*, kemudian teknologi misalnya seperti *server* dan *network* yang harus kita lindungi.

Kemudian How, bagaimana cara melindunginya. Dalam cyber security ada istilah *cyber security function*, ada area fungsi *preventative, detective*, dan *corrective*. Kita melindungi data kita dengan sistem menggunakan *firewall* atau *antivirus*, detectivenya kita pasang *monitoring* seperti itu, *corrective-nya* salah satu contoh Pentest VA sehingga nanti ditemukan *finding* dan melakukan perbaikan. Kemudian Who, semua punya tanggung jawab di area masing masing. Kalau When, harus berulang dilakukan secara berkala, seperti itu.

Kalau dari point of view cyber security expert, bagaimana cara dalam mem-bantu perusahaan dan bisnis?

Tim *cyber security* meng-enable itu semua, dan tantangannya itu. kalau berbicara soal manusianya, sekarang kita paling sering mendengar *security awareness* ya, tapi sekarang bukan lagi jamannya itu melainkan *security culture* dimana kita membangun budaya keamanan informasi. User punya resiko diserang karena dia punya otorisasi data, namun tidak kalah pentingnya, developer-developer yang punya source code juga punya resiko diserang. Itulah tantangannya meng-enable itu semua sesuai dengan 5W 1H tadi. Sehingga entry pointnya untuk kita, tim *cyber security* adalah menanamkan kesadaran bahwa semua punya peran penting dalam menjaga keamanan informasi. Makanya kita melakukan simulasi-simulasi supaya semua menyadari bahayanya kalau sampai dijebol seperti ini, misalnya seperti itu.

Jadi dari sisi infrastruktur kita bisa membantu melakukan sisi assessment dari security infrastruktur tersebut. Kalau dari sisi manusianya, mengenable pola pikir sisi *cyber security*-nya.

Apakah ada pesan-pesan yang bisa diberikan untuk para pembaca terkait dengan cyber security ini?

Pesan dari kami, intinya kita sama-sama menjaga. Tujuannya supaya bisnis bisa berjalan lancar, reputasi bagus dan bisa mencapai kesuksesan bersama. Kita saling menjaga keamanan informasi supaya perusahaan bisa terus berkembang dan sukses. Analoginya, tim cyber security adalah tentaranya dan rekan-rekan adalah rakyatnya. Keamanan suatu negara bukan hanya dari tentaranya saja tapi juga bersama dengan rakyat, karena kalau kompak maka kita semua akan kuat. Kita memiliki tanggung jawab untuk mengamankan diri serta data perusahaan. Serta jangan pernah merasa aman karena bisa saja anda menjadi sasaran. So, always enabling your secrity awareness.

“One single vulnerability is all an attacker needs.”

Window Snyder,
Chief Security Officer, Fastly

What Xapiens can do?

Xapiens memiliki cyber security sebagai salah satu bisnis pillar di perusahaan untuk klien yang membutuhkan support ataupun mengalami kendala dari sisi *cyber security-nya*. Dimana layanan cyber security di Xapiens mencakup scope, mulai dari vulnerability assessments & Penetration testing (VAPT), hingga security awareness program. Xapiens membagi layanan cyber security ini ke dalam 3 tipe produk yaitu red team, blue team, dan purple team. Xapiens juga memiliki *cyber security* team yang berkompeten di bidangnya yang dapat mendukung Xapiens dalam upayanya memberikan layanan yang baik serta kompetitif di pasaran. Sekarang pertanyaannya, apa yang kami bisa bantu untuk perlindungan siber usaha anda?
(HSP)

Apabila anda tertarik ingin mengkonfirmasi dan mengenal lebih jauh layanan kami, silahkan hubungi **(+62)21 2977 0900** atau email kami di **Hello@xapiens.id**

Red Team	Blue Team	Purple Team
Vulnerability Assessment	SOC	Security Awareness Program: • Phishing Simulation • Webinar workshop • Online Based Security Training • Security Awareness Campaign
Penetration Testing	Threat Intelligence Services	
Physical Pentest	IT Security Hardening	
	Digital / Computer Forensic	

Introduction to AWS Services Webinar

Dwi Fahni Denni, Infrastructure and Cloud Manager Xapiens Teknologi Indonesia pada 9 September lalu, menjadi pembicara dalam sesi webinar bersama dengan AWS community. Webinar yang bertajuk "Introduction to AWS Services" ini membahas seputar Amazon Web Services dan penerapannya di dalam perusahaan.

Amazon Web Services (AWS) sendiri merupakan penyedia layanan cloud yang aman dan telah digunakan secara luas di dunia, termasuk startup. AWS menawarkan lebih dari 200 layanan unggulan yang lengkap dari pusat data secara global. Jika anda memiliki kebutuhan terkait solusi AWS, silahkan hubungi di ***Hello@Xapiens.id.***

Xapiens New Partner: Red Hat

Xapiens pada bulan september ini berhasil mendapatkan pencapaian baru dalam hubungan partnership, yang mana Xapiens secara resmi telah menjadi Red Hat Ready Partner. Red Hat merupakan perusahaan yang bergerak di bidang software, yang menyediakan open-source *software* product untuk solusi IT enterprise.

Ini merupakan salah satu bentuk upaya kami dalam rangka senantiasa ber-inovasi demi kemajuan bisnis perusahaan, salah satunya di bidang partnership. Adanya kerjasama dengan Red Hat sebagai ready partner, harapannya dapat mendukung Xapiens dalam memberikan layanan yang lebih baik dan kompetitif untuk klien Xapiens, baik internal maupun eksternal.