setiap kelompok memilih kasus data breach dan dijelaskan

2021 Microsoft Exchange Server Data Breach

Nama Anggota Kelompok :
1. Nanda S. Prawira
2. Rahmi
3. Rani Okta Felani

Latar Belakang

Serangan dunia maya dan pelanggaran data dimulai pada Januari 2021, setelah melalui empat ekspliotasi di temukan server Microsoft Exchange Lokal. Yang memberikan penyerang akses penuh ke email dan kata sandi pengguna di server yang terpengaruh, hak istimewa administrator di server, dan akses ke perangkat yang terhubung di jaringan yang sama. Penyerangan biasa nya dilakukan melalui pintu belakang yang memungkinkan penyerang mengakses penuh ke server yang terkena dampak bahkan jika nanti server di perbaharui agar tidak lagi rentan terhadap eksploitasi. Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF).

Microsoft exchange dianggap sebagai target bernilai tinggi bagi peretas yang ingin menembus jaringan bisnis, karena ini adalah perangkat lunak server email, dan menurut microsoft ini menyediakan lingkungan unik yang memungkinkan penyerang melakukan berbagai tugas menggunakan perangkat bawaan yang sama.

Pada 5 Januari 2021, perusahaan penguji keamanan DEVCORE membuat laporan paling awal tentang kerentanan ke Microsoft, yang diverifikasi Microsoft pada 8 Januari. Pelanggaran pertama dari instans Microsoft Exchange Server diamati oleh perusahaan keamanan siber Volexity pada 6 Januari 2021. Pada akhir Januari, perusahaan keamanan siber Volexity telah mengamati pelanggaran yang memungkinkan penyerang untuk memata-matai dua pelanggan mereka, dan memberi tahu Microsoft tentang kerentanan. Setelah Microsoft diberi tahu tentang pelanggaran tersebut, Volexity mencatat bahwa peretas menjadi tidak terlalu sembunyi-sembunyi untuk mengantisipasi adanya tambalan.

Pada 2 Maret 2021, perusahaan keamanan siber lain, ESET , menulis bahwa mereka mengamati beberapa penyerang selain Hafnium yang mengeksploitasi kerentanan. Wired melaporkan pada 10 Maret bahwa sekarang setelah kerentanan telah ditambal, lebih banyak penyerang akan merekayasa balik perbaikan tersebut untuk mengeksploitasi server yang masih rentan. Analis di dua perusahaan keamanan melaporkan mereka mulai melihat bukti bahwa penyerang sedang bersiap untuk menjalankan perangkat lunak cryptomining di server.

Pada 10 Maret 2021, peneliti keamanan Nguyen Jang memposting kode bukti konsep ke GitHub milik Microsoft tentang cara kerja exploit, dengan total 169 baris kode; Program ini sengaja ditulis dengan kesalahan sehingga sementara peneliti keamanan dapat memahami cara kerja eksploitasi, pelaku jahat tidak akan dapat menggunakan kode tersebut untuk mengakses server. Kemudian pada hari itu, GitHub menghapus kode tersebut karena "berisi bukti kode konsep untuk kerentanan yang baru-baru ini diungkapkan yang sedang dieksploitasi secara aktif". Pada tanggal 13 Maret, grup lain secara independen menerbitkan kode eksploitasi, dengan kode ini memerlukan modifikasi minimal untuk bekerja; yang Koordinasi Pusat CERTWill Dormann mengatakan "eksploitasi benar-benar keluar dari kantong sekarang" sebagai tanggapan.

Serangan itu terjadi tak lama setelah pelanggaran data pemerintah federal Amerika Serikat tahun 2020 , yang juga menyebabkan aplikasi web dan rantai pasokan Microsoft Outlook dikompromikan . Microsoft mengatakan tidak ada hubungan antara kedua insiden tersebut.

Tujuan

Microsoft mengidentifikasi Hafnium sebagai "aktor yang sangat terampil dan canggih" yang secara historis sebagian besar menargetkan "entitas di Amerika Serikat untuk tujuan mengekstrak informasi dari sejumlah sektor industri, termasuk peneliti penyakit menular, firma hukum, lembaga pendidikan tinggi , kontraktor pertahanan, lembaga pemikir kebijakan, dan LSM. " Mengumumkan peretasan tersebut, Microsoft menyatakan bahwa ini adalah "kali kedelapan dalam 12 bulan terakhir ini Microsoft telah secara terbuka mengungkapkan kelompok negara-bangsa yang menargetkan lembaga yang penting bagi masyarakat sipil." Pada 12 Maret 2021, ada, selain Hafnium, setidaknya sembilan kelompok berbeda lainnya yang mengeksploitasi kerentanan, masing-masing dengan gaya dan prosedur berbeda.

Peretas mengambil keuntungan dari empat kerentanan zero-day yang terpisah untuk mengganggu Outlook Web Access (OWA) server Microsoft Exchange , memberi mereka akses ke seluruh server dan jaringan korban serta ke email dan undangan kalender, hanya di pertama-tama memerlukan alamat server, yang dapat ditargetkan secara langsung atau diperoleh dengan pemindaian massal untuk server yang rentan; penyerang kemudian menggunakan dua eksploitasi, yang pertama mengizinkan penyerang untuk terhubung ke server dan melakukan otentikasi palsu sebagai pengguna standar. Dengan itu, kerentanan kedua kemudian dapat dieksploitasi, meningkatkan akses pengguna tersebut ke hak administrator . Dua eksploitasi terakhir memungkinkan penyerang untuk mengunggah kode ke server di lokasi mana pun yang mereka inginkan, yang secara otomatis berjalan dengan hak administrator ini. Penyerang kemudian biasanya menggunakan ini untuk menginstal shell web , menyediakan pintu belakang ke server yang disusupi, yang memberikan akses berkelanjutan kepada peretas ke server selama kedua shell web tetap aktif dan server Exchange tetap aktif.

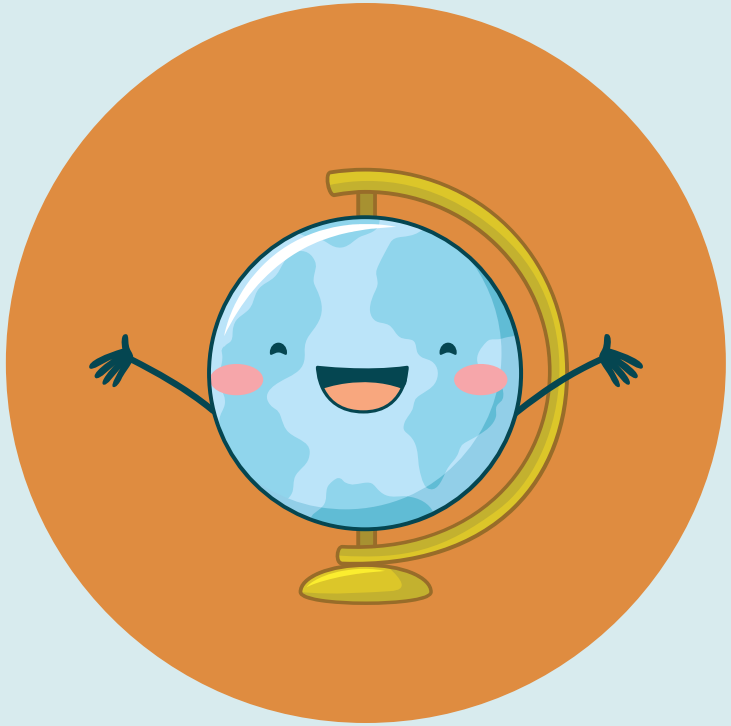
Kerugian

Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF).

wakil presiden Microsoft untuk Keamanan & Kepercayaan Pelanggan, menulis bahwa target mencakup peneliti penyakit, kantor hukum, universitas, kontraktor pertahanan, organisasi non-pemerintah , dan lembaga pemikir .

Check Point Research telah mengamati Amerika Serikat sebagai negara yang paling banyak diserang dengan 17% dari semua upaya eksploitasi, diikuti oleh Jerman dengan 6%, Inggris dan Belanda keduanya di 5%, dan Rusia dengan 4% dari semua eksploitasi; pemerintah / militer adalah sektor yang paling ditargetkan dengan 23% upaya eksploitasi, diikuti oleh manufaktur sebesar 15%, layanan perbankan dan keuangan sebesar 14%, vendor perangkat lunak dengan 7% dan perawatan kesehatan sebesar 6%

Pada 12 Maret 2021, Intelijen Keamanan Microsoft mengumumkan "keluarga baru ransomware " yang disebut DearCry sedang disebarkan ke server yang awalnya terinfeksi, mengenkripsi konten perangkat, membuat server tidak dapat digunakan, dan menuntut pembayaran untuk memulihkan file. Pada 18 Maret 2021, afiliasi ransomware cybergang REvil mengklaim bahwa mereka telah mencuri data tidak terenkripsi dari perusahaan perangkat keras dan elektronik Taiwan Acer , termasuk sejumlah perangkat yang dirahasiakan yang sedang dienkripsi, dengan firma keamanan siber Advanced Intel menautkan pelanggaran

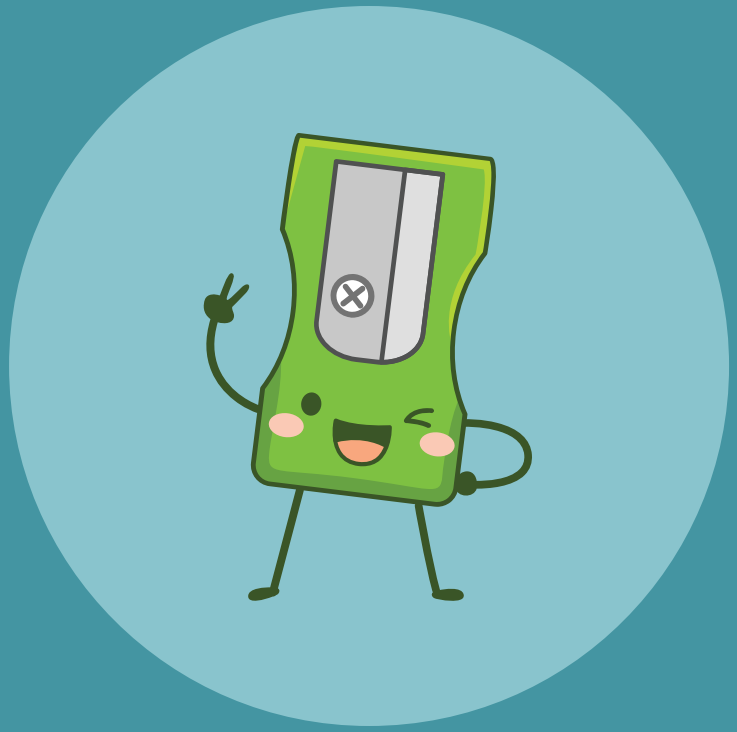


Kesimpulan & Saran

Pada 2 Maret 2021, Pusat Respons Keamanan Microsoft (MSRC) secara publik memposting rilis Common Vulnerabilities and Exposures (CVE) out-of-band , mendesak kliennya untuk menambal server Exchange mereka untuk mengatasi sejumlah kerentanan kritis . Pada tanggal 15 Maret, Microsoft merilis alat PowerShell sekali klik , Alat Mitigasi Exchange On-Premises, yang menginstal pembaruan spesifik yang melindungi dari ancaman, menjalankan pemindaian malware yang juga mendeteksi shell web yang diinstal, dan menghapus ancaman yang terdeteksi; ini direkomendasikan sebagai tindakan mitigasi sementara, karena tidak menginstal pembaruan lain yang tersedia.

Pada 3 Maret 2021, Cybersecurity and Infrastructure Security Agency (CISA) AS mengeluarkan arahan darurat yang memaksa jaringan pemerintah untuk memperbarui ke versi Exchange yang ditambal. Pada 8 Maret, CISA men-tweet apa yang NBC News gambarkan sebagai "pesan yang tidak biasa" mendesak "SEMUA organisasi di SEMUA sektor" untuk mengatasi kerentanan.

Badan resmi lainnya yang mengungkapkan keprihatinan termasuk Gedung Putih , Otoritas Keamanan Nasional Norwegia, dan Kantor Keamanan Cyber dan Informasi Republik Ceko. Pada 7 Maret 2021, CNN melaporkan bahwa pemerintahan Biden diharapkan membentuk satuan tugas untuk mengatasi pelanggaran tersebut; pemerintahan Biden telah mengundang organisasi sektor swasta untuk berpartisipasi dalam gugus tugas dan akan memberi mereka informasi rahasia yang dianggap perlu. Penasihat Keamanan Nasional AS Jake Sullivan menyatakan bahwa AS belum dalam posisi untuk disalahkan atas serangan itu.



TERIMAKASIH

ASSALAMMUALAIKUM ☺

KASUS KEBOCORAN DATA PENGGUNA TOKOPEDIA

TUGAS KELOMPOK

IT AUDIT

OLEH :

SIGIT PAMUNGKAS (192420047)

SUWANI (192420049)

THEO VHALDINO (192420058)

YAYAN CANDRA SUBIDIN (192420054)

PROGRAM STUDI TEKNIK INFORMATIKA S-2

PROGRAM PASCA SARJANA

UNIVERSITAS BINA DARMA

2021

I. Latar Belakang

Pada awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan. Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020. Kendati membenarkan adanya upaya pencurian,Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun. bocornya 91 juta data pengguna. Aksi pencurian ini dilakukan hacker bernama samaran Shiny Hunter. William Tanuwijaya mengungkapkan Tokopedia menyadari adanya pencurian data oleh pihak Ketiga yang tidak bertanggung jawab pada 2 Mei 2020. Setelahnya pihaknya mengambil tiga tindakan. *Pertama*, langsung memberikan informasi kepada seluruh pengguna Tokopedia, memulai proses investigasi dan mengambil langkah-langkah yang perlu dilakukan untuk memastikan akun dan transaksi tetap terjaga.

Kedua, kami telah berkomunikasi dan bekerja sama dengan pemerintah, antara lain Kementerian Komunikasi dan Informatika serta Badan Siber dan Sandi Negara untuk melakukan investigasi atas kejadian ini sekaligus memastikan keamanan dan perlindungan atas data pribadi Anda.

Ketiga, selain melakukan investigasi internal dengan teliti, kami juga telah menunjuk institusi independen kelas dunia yang memiliki spesialisasi di bidang keamanan siber dalam membantu investigasi dan identifikasi langkah-langkah yang diperlukan guna lebih meningkatkan lagi perlindungan data para pengguna Tokopedia.

II. Manfaat hacker

Manfaat yang diperoleh hacker membobol data pengguna toko pedia ialah :

1. Mendapatkan data
2. Menyalahgunakan data
3. Menjual data.

Dapat bersifat pribadi dapat saja di gunakan untuk hal kejahatan dalam bidang IT.

III. Kerugian yang didapat tokopedia

1. Reputasi perusahaan tentunya menurun drastis dan membuat kurangnya kepercayaan pelanggan terhadap perusahaan
2. Finansial
3. Hukuman regulasi jika tidak ditanggulangi dengan tepat

IV. Solusi :

Apabila jika pemrosesan data ditangani secara efektif, kerusakan dari potensi pelanggaran data pelanggan dapat dikurangi secara signifikan. Adapun beberapa cara untuk menangani pembocoran datasebagai berikut :

1. Gunakan pelatihan dan aktivitas yang akan mendidik karyawan tentang dasar-dasar keamanan siber, misalnya, untuk tidak membuka atau menyimpan file dari email atau situs web yang tidak dikenal karena dapat membahayakan seluruh perusahaan;
2. Ingatkan karyawan secara rutin tentang cara menangani data sensitif, misalnya, untuk menyimpan hanya di layanan cloud tepercaya dengan autentikasi diaktifkan, jangan membagikannya dengan pihak ketiga yang tidak tepercaya;
3. Terapkan penggunaan perangkat lunak yang sah, diunduh dari sumber resmi;

4. Buat cadangan data penting dan perbarui peralatan serta aplikasi TI secara teratur untuk menghindari kerentanan yang belum ditambal yang dapat menjadi penyebab kebocoran.
5. Gunakan produk titik akhir khusus yang menuntut manajemen minimum yang memungkinkan karyawan melakukan pekerjaan utama mereka, namun tetap terlindung dari malware, ransomware, pengambilalihan akun, penipuan online, dan penipuan, seperti Kaspersky Endpoint Security for Business.

Adapun saran lain menurut Kaspersky:

1. Memberi tim Pusat Operasi Keamanan (SOC) di perusahaan akses ke intelijen ancaman terbaru, dan tetap mengikuti perkembangan alat, teknik, dan taktik baru yang sedang berkembang yang digunakan oleh aktor ancaman dan pelaku kejahatan siber;
2. Untuk deteksi level endpoint, investigasi, dan remediasi insiden tepat waktu, terapkan solusi EDR (Endpoint Detection and Response);
3. Selain mengadopsi perlindungan titik akhir yang penting, terapkan pula solusi keamanan tingkat perusahaan untuk mendeteksi ancaman tingkat lanjut di tingkat jaringan pada tahap awal.

Pengguna kami adalah prioritas utama. Maka dari itu, sebagai langkah pencegahan tambahan, kami senantiasa mengajak seluruh pengguna Tokopedia mengikuti anjuran langkah pengamanan agar semua tetap terlindungi, seperti memastikan bahwa Anda selalu mengganti kata sandi akun Tokopedia secara berkala, tidak menggunakan kata sandi yang sama di berbagai platform digital, dan menjaga OTP dengan tidak memberikan kode OTP tersebut kepada pihak manapun termasuk yang mengatasnamakan Tokopedia dan untuk alasan apapun.

KASUS KEBOCORAN DATA PENGGUNA TOKOPEDIA

TUGAS KELOMPOK

IT AUDIT

OLEH :

SIGIT PAMUNGKAS (192420047)

SUWANI (192420049)

THEO VHALDINO (192420058)

YAYAN CANDRA SUBIDIN (192420054)

PROGRAM STUDI TEKNIK INFORMATIKA S-2

PROGRAM PASCA SARJANA

UNIVERSITAS BINA DARMA

2021

I. Latar Belakang

Pada awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan. Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020. Kendati membenarkan adanya upaya pencurian,Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun. bocornya 91 juta data pengguna. Aksi pencurian ini dilakukan hacker bernama samaran Shiny Hunter. William Tanuwijaya mengungkapkan Tokopedia menyadari adanya pencurian data oleh pihak Ketiga yang tidak bertanggung jawab pada 2 Mei 2020. Setelahnya pihaknya mengambil tiga tindakan. *Pertama,* langsung memberikan informasi kepada seluruh pengguna Tokopedia, memulai proses investigasi dan mengambil langkah-langkah yang perlu dilakukan untuk memastikan akun dan transaksi tetap terjaga.

Kedua, kami telah berkomunikasi dan bekerja sama dengan pemerintah, antara lain Kementerian Komunikasi dan Informatika serta Badan Siber dan Sandi Negara untuk melakukan investigasi atas kejadian ini sekaligus memastikan keamanan dan perlindungan atas data pribadi Anda.

Ketiga, selain melakukan investigasi internal dengan teliti, kami juga telah menunjuk institusi independen kelas dunia yang memiliki spesialisasi di bidang keamanan siber dalam membantu investigasi dan identifikasi langkah-langkah yang diperlukan guna lebih meningkatkan lagi perlindungan data para pengguna Tokopedia.

II. Manfaat yang di dapat hacker

Manfaat yang diperoleh hacker membobol data pengguna toko pedia ialah :

1. Mendapatkan data
2. Menyalahgunakan data
3. Menjual data.

Dapat bersifat pribadi dapat saja di gunakan untuk hal kejahatan dalam bidang IT.

III. Kerugian yang didapat tokopedia

1. Reputasi perusahaan tentunya menurun drastis dan membuat kurangnya kepercayaan pelanggan terhadap perusahaan
2. Finansial
3. Hukuman regulasi jika tidak ditanggulangi dengan tepat
4. Hilangnya kepercayaan pelanggan terhadap perusahaan.

IV. Cara Menanggulangi/ Pencegahan

Apabila jika pemrosesan data ditangani secara efektif, kerusakan dari potensi pelanggaran data pelanggan dapat dikurangi secara signifikan. Adapun beberapa cara untuk menangani pembocoran datasebagai berikut :

1. Gunakan pelatihan dan aktivitas yang akan mendidik karyawan tentang dasar-dasar keamanan siber, misalnya, untuk tidak membuka atau menyimpan file dari email atau situs web yang tidak dikenal karena dapat membahayakan seluruh perusahaan;
2. Ingatkan karyawan secara rutin tentang cara menangani data sensitif, misalnya, untuk menyimpan hanya di layanan cloud tepercaya dengan autentikasi diaktifkan, jangan membagikannya dengan pihak ketiga yang tidak tepercaya;
3. Terapkan penggunaan perangkat lunak yang sah, diunduh dari sumber resmi;
4. Buat cadangan data penting dan perbarui peralatan serta aplikasi TI secara teratur untuk menghindari kerentanan yang belum ditambal yang dapat menjadi penyebab kebocoran.
5. Gunakan produk titik akhir khusus yang menuntut manajemen minimum yang memungkinkan karyawan melakukan pekerjaan utama mereka, namun tetap terlindung

dari malware, ransomware, pengambilalihan akun, penipuan online, dan penipuan, seperti Kaspersky Endpoint Security for Business.

Adapun saran lain menurut Kaspersky:

1. Memberi tim Pusat Operasi Keamanan (SOC) di perusahaan akses ke intelijen ancaman terbaru, dan tetap mengikuti perkembangan alat, teknik, dan taktik baru yang sedang berkembang yang digunakan oleh aktor ancaman dan pelaku kejahatan siber;
2. Untuk deteksi level endpoint, investigasi, dan remediasi insiden tepat waktu, terapkan solusi EDR (Endpoint Detection and Response);
3. Selain mengadopsi perlindungan titik akhir yang penting, terapkan pula solusi keamanan tingkat perusahaan untuk mendeteksi ancaman tingkat lanjut di tingkat jaringan pada tahap awal.

Pengguna kami adalah prioritas utama. Maka dari itu, sebagai langkah pencegahan tambahan, kami senantiasa mengajak seluruh pengguna Tokopedia mengikuti anjuran langkah pengamanan agar semua tetap terlindungi, seperti memastikan bahwa Anda selalu mengganti kata sandi akun Tokopedia secara berkala, tidak menggunakan kata sandi yang sama di berbagai platform digital, dan menjaga OTP dengan tidak memberikan kode OTP tersebut kepada pihak manapun termasuk yang mengatasnamakan Tokopedia dan untuk alasan apapun.

Sumber Berita

https://www.cnbcindonesia.com/tech/20200512133506-37-157889/buka-bukaan-bos-tokopedia-soal-bocornya-91-juta-data-pengguna

https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020?page=all

KASUS KEBOCORAN DATA PENGGUNA TOKOPEDIA

TUGAS KELOMPOK

IT AUDIT

OLEH :

SIGIT PAMUNGKAS (192420047)

SUWANI (192420049)

THEO VHALDINO (192420058)

YAYAN CANDRA SUBIDIN (192420054)

PROGRAM STUDI TEKNIK INFORMATIKA S-2

PROGRAM PASCA SARJANA

UNIVERSITAS BINA DARMA

2021

I. Latar Belakang

Pada awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan. Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020. Kendati membenarkan adanya upaya pencurian,Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun. bocornya 91 juta data pengguna. Aksi pencurian ini dilakukan hacker bernama samaran Shiny Hunter. William Tanuwijaya mengungkapkan Tokopedia menyadari adanya pencurian data oleh pihak Ketiga yang tidak bertanggung jawab pada 2 Mei 2020. Setelahnya pihaknya mengambil tiga tindakan. *Pertama,* langsung memberikan informasi kepada seluruh pengguna Tokopedia, memulai proses investigasi dan mengambil langkah-langkah yang perlu dilakukan untuk memastikan akun dan transaksi tetap terjaga.

Kedua, kami telah berkomunikasi dan bekerja sama dengan pemerintah, antara lain Kementerian Komunikasi dan Informatika serta Badan Siber dan Sandi Negara untuk melakukan investigasi atas kejadian ini sekaligus memastikan keamanan dan perlindungan atas data pribadi Anda.

Ketiga, selain melakukan investigasi internal dengan teliti, kami juga telah menunjuk institusi independen kelas dunia yang memiliki spesialisasi di bidang keamanan siber dalam membantu investigasi dan identifikasi langkah-langkah yang diperlukan guna lebih meningkatkan lagi perlindungan data para pengguna Tokopedia.

II. Manfaat yang di dapat hacker

Manfaat yang diperoleh hacker membobol data pengguna toko pedia ialah :

1. Mendapatkan data
2. Menyalahgunakan data
3. Menjual data.

Dapat bersifat pribadi dapat saja di gunakan untuk hal kejahatan dalam bidang IT.

III. Kerugian yang didapat tokopedia

1. Reputasi perusahaan tentunya menurun drastis dan membuat kurangnya kepercayaan pelanggan terhadap perusahaan
2. Finansial
3. Hukuman regulasi jika tidak ditanggulangi dengan tepat
4. Hilangnya kepercayaan pelanggan terhadap perusahaan.

IV. Cara Menanggulangi/ Pencegahan

Apabila jika pemrosesan data ditangani secara efektif, kerusakan dari potensi pelanggaran data pelanggan dapat dikurangi secara signifikan. Adapun beberapa cara untuk menangani pembocoran datasebagai berikut :

1. Gunakan pelatihan dan aktivitas yang akan mendidik karyawan tentang dasar-dasar keamanan siber, misalnya, untuk tidak membuka atau menyimpan file dari email atau situs web yang tidak dikenal karena dapat membahayakan seluruh perusahaan;
2. Ingatkan karyawan secara rutin tentang cara menangani data sensitif, misalnya, untuk menyimpan hanya di layanan cloud tepercaya dengan autentikasi diaktifkan, jangan membagikannya dengan pihak ketiga yang tidak tepercaya;
3. Terapkan penggunaan perangkat lunak yang sah, diunduh dari sumber resmi;
4. Buat cadangan data penting dan perbarui peralatan serta aplikasi TI secara teratur untuk menghindari kerentanan yang belum ditambal yang dapat menjadi penyebab kebocoran.
5. Gunakan produk titik akhir khusus yang menuntut manajemen minimum yang memungkinkan karyawan melakukan pekerjaan utama mereka, namun tetap terlindung

dari malware, ransomware, pengambilalihan akun, penipuan online, dan penipuan, seperti Kaspersky Endpoint Security for Business.

Adapun saran lain menurut Kaspersky:

1. Memberi tim Pusat Operasi Keamanan (SOC) di perusahaan akses ke intelijen ancaman terbaru, dan tetap mengikuti perkembangan alat, teknik, dan taktik baru yang sedang berkembang yang digunakan oleh aktor ancaman dan pelaku kejahatan siber;
2. Untuk deteksi level endpoint, investigasi, dan remediasi insiden tepat waktu, terapkan solusi EDR (Endpoint Detection and Response);
3. Selain mengadopsi perlindungan titik akhir yang penting, terapkan pula solusi keamanan tingkat perusahaan untuk mendeteksi ancaman tingkat lanjut di tingkat jaringan pada tahap awal.

Pengguna kami adalah prioritas utama. Maka dari itu, sebagai langkah pencegahan tambahan, kami senantiasa mengajak seluruh pengguna Tokopedia mengikuti anjuran langkah pengamanan agar semua tetap terlindungi, seperti memastikan bahwa Anda selalu mengganti kata sandi akun Tokopedia secara berkala, tidak menggunakan kata sandi yang sama di berbagai platform digital, dan menjaga OTP dengan tidak memberikan kode OTP tersebut kepada pihak manapun termasuk yang mengatasnamakan Tokopedia dan untuk alasan apapun.

Sumber Berita

https://www.cnbcindonesia.com/tech/20200512133506-37-157889/buka-bukaan-bos-tokopedia-soal-bocornya-91-juta-data-pengguna

https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020?page=all

KASUS DATA BRACH
PADA TOKOPEDIA DI AWAL MEI 2020

DISUSUN OLEH :

ELPINA SARI (192420050)

ARFA FAUZIAH (192420055)

AL-ADRI NOFA GUSANDI (192420053)

Latar Belakang

- Perkembangan dunia teknologi saat ini sangat cepat, sehingga manusia dituntut untuk mengikuti perkembangan. Untuk itu dibutuhkan sumber daya manusia dalam bidang IT yang memiliki kemampuan beradaptasi secara cepat. Dalam dunia teknologi informasi saat ini kebutuhan terhadap data adalah sebuah kunci yang wajib dimiliki pada setiap lini bisnis.
- Besarnya data yang tersimpan di dalam sebuah perusahaan berkembang sangat cepat tiap harinya. Kemampuan untuk mengakses dan menganalisa data tersebut dalam pembuatan keputusan yang cepat dan cerdas menjadi kunci kesuksesan sebuah perusahaan. Data tersebut disimpan dalam lokasi, sistem, format dan skema yang berbeda dan memberikan tantangan dalam penggunaan maupun integrasinya
- Sepanjang tahun 2020, muncul rentetan kasus kebocoran data baik yang dialami pemerintah maupun perusahaan swasta seperti platform e-commerce. Kasus kebocoran data ini terjadi mulai bulan Mei 2020. Dalam kasus kebocoran tersebut, peretas mencuri data pengguna lalu menjualnya ke forum gelap.
- Pada tugas ini penulis akan membahas tentang apa penyebab kebocoran data pada situs Toko Pedia tersebut dan bagaimana cara melakukan pencegahannya

PEMBAHASAN

- **Data Breach**

Menurut Wikipedia.org (2021), Pelanggaran data adalah pelepasan informasi aman atau pribadi / rahasia yang disengaja atau tidak disengaja ke lingkungan yang tidak tepercaya. Istilah lain untuk fenomena ini antara lain keterbukaan informasi yang tidak disengaja, kebocoran data, kebocoran informasi dan juga tumpahan data. Insiden berkisar dari serangan bersama oleh topi hitam, atau individu yang meretas untuk keuntungan pribadi, terkait dengan kejahatan terorganisir, aktivis politik atau pemerintah nasional hingga pembuangan peralatan komputer bekas atau media penyimpanan data secara sembarangan dan sumber yang tidak dapat diretas.

Penyebab Kebocoran Data Pada Toko Pedia

- Awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan.
- Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020.
- Kendati membenarkan adanya upaya pencurian, Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun.

Cara Pencegahan pembobolan akun e-commers

- Dikabarkan bahwa data dari 91 juta pengguna Tokopedia telah berhasil diambil dan dijual di dark web seharga 76 juta Rupiah.
- Menteri Komunikasi dan Informatika (Menkominfo), Johnny G. Plate juga sudah memberikan tanggapan terkait masalah ini.
- Menteri Johnny mengatakan bahwa Kemenkominfo akan secara serius melakukan evaluasi, penyelidikan, dan mitigasi teknis.
- Pihak kementerian terkait juga melakukan kerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk menangani kebocoran data e-commerce ini.
- Namun, sebagai pengguna, tentunya kita juga harus melakukan beberapa antisipasi sebelum pihak berwenang yang melakukannya.
- Nextren telah memiliki beberapa cara yang mungkin bisa menjadi tindakan pencegahannya.

Berikut langkah-langkah yang kamu bisa lakukan :

1. **Aktifkan Update Otomatis**
2. **Ubah Password**
3. **Lapor ke Pihak E-Commerce**
4. **Aktifkan Two-Factor Authentication**
5. **Tidak Menyimpan Akun Pembayaran**

DAFTAR PUSTAKA

Nengsih Warnia. 2019 : Implementasi Data Mining

Pane, Syafrial Fachri. 2020 : Big data classification behavior menggunakan python

https://en.m.wikipedia.org/wiki/Unstructured_data

https://id.quora.com/Apa-perbedaan-antara-data-terstruktur-dan-tidak-terstruktur

KASUS DATA BRACH

PADA TOKO PEDIA DI AWAL MEI 2020

OLEH :

ALADRI NOFA GUSANDI

ARPA PAUZIAH

ELPINA SARI

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

2020/2021

1. Pendahuluan

Perkembangan dunia teknologi saat ini sangat cepat, sehingga manusia dituntut untuk mengikuti perkembangan. Untuk itu dibutuhkan sumber daya manusia dalam bidang IT yang memiliki kemampuan beradaptasi secara cepat. Dalam dunia teknologi informasi saat ini kebutuhan terhadap data adalah sebuah kunci yang wajib dimiliki pada setiap lini bisnis. Meskipun bisnisnya bahkan tidak berhubungan dengan dunia teknologi, namun data sangat diperlukan dalam melakukan analisis yang nantinya akan digunakan untuk pengambilan keputusan.

Besarnya data yang tersimpan di dalam sebuah perusahaan berkembang sangat cepat tiap harinya. Kemampuan untuk mengakses dan menganalisa data tersebut dalam pembuatan keputusan yang cepat dan cerdas menjadi kunci kesuksesan sebuah perusahaan. Banyak perusahaan yang terus berkembang seiring dengan berputarnya waktu, sehingga menghasilkan informasi yang heterogen dari data yang terdistribusi di berbagai sumber. Data tersebut disimpan dalam lokasi, sistem, format dan skema yang berbeda dan memberikan tantangan dalam penggunaan maupun integrasinya.

Sepanjang tahun 2020, muncul rentetan kasus kebocoran data baik yang dialami pemerintah maupun perusahaan swasta seperti platform e-commerce. Kasus kebocoran data ini terjadi mulai bulan Mei 2020. Dalam kasus kebocoran tersebut, peretas mencuri data pengguna lalu menjualnya ke forum gelap.

Pada tugas ini penulis akan membahas tentang apa penyebab kebocoran data pada situs Toko Pedia tersebut dan bagaimana cara melakukan pencegahannya.

2. PEMBAHASAN

1. Data Breach

Menurut Wikipedia.org (2021), Pelanggaran data adalah pelepasan informasi aman atau pribadi / rahasia yang disengaja atau tidak disengaja ke lingkungan yang tidak tepercaya. Istilah lain untuk fenomena ini antara lain keterbukaan informasi yang tidak disengaja, kebocoran data, kebocoran informasi dan juga tumpahan data. Insiden berkisar dari serangan bersama oleh topi hitam, atau individu yang meretas untuk keuntungan pribadi, terkait dengan kejahatan terorganisir, aktivis politik atau pemerintah nasional hingga pembuangan peralatan komputer bekas atau media penyimpanan data secara sembarangan dan sumber yang tidak dapat diretas.

2. Penyebab Kebocoran Data Pada Toko Pedia

Awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan.

Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020.

Kendati membenarkan adanya upaya pencurian, Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun.

3. Cara Pencegahan pembobolan akun e-commers

Dikabarkan bahwa data dari 91 juta pengguna Tokopedia telah berhasil diambil dan dijual di dark web seharga 76 juta Rupiah.

Menteri Komunikasi dan Informatika (Menkominfo), Johnny G. Plate juga sudah memberikan tanggapan terkait masalah ini.

Menteri Johnny mengatakan bahwa Kemenkominfo akan secara serius melakukan evaluasi, penyelidikan, dan mitigasi teknis.

Pihak kementerian terkait juga melakukan kerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk menangani kebocoran data e-commerce ini.

Namun, sebagai pengguna, tentunya kita juga harus melakukan beberapa antisipasi sebelum pihak berwenang yang melakukannya.

Nextren telah memiliki beberapa cara yang mungkin bisa menjadi tindakan pencegahannya.

Berikut langkah-langkah yang kamu bisa lakukan!

1. Aktifkan Update Otomatis

Langkah pertama yang bisa kamu lakukan adalah pengaktifan update secara otomatis pada aplikasi.

Hal ini menjadi alternatif pertama karena kamu bisa dengan cepat mendapatkan versi terbaru dari aplikasi.

Pembaruan aplikasi biasanya tidak hanya dari segi fitur, namun juga dari sisi keamanannya.

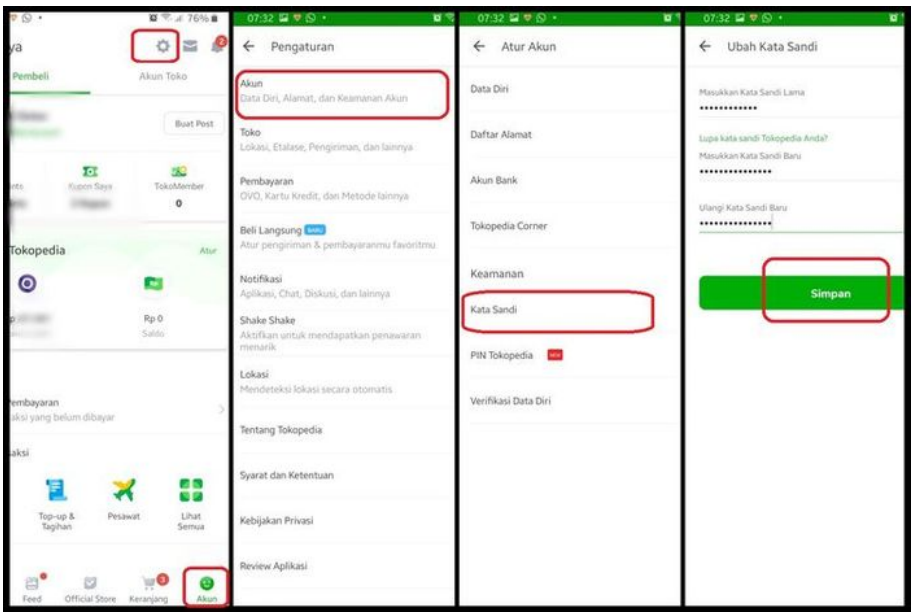
Untuk itu, cara ini Nextren anggap perlu untuk dilakukan oleh para pengguna e-commerce.

2. Ubah Password

Cara kedua yang bisa kalian gunakan untuk mengamankan data kalian adalah mengubah password.

Langkah ini memang cukup klasik, namun mengubah password dapat membuat data kamu bisa lebih aman dari para hacker.

Pihak Tokopedia sebagai perusahaan yang mengalami serangan hacker juga sempat menyarankan kepada penggunanya untuk mengganti password.



Jangan lupa juga membuat password yang unik dari setiap akun yang memasukkan data pribadimu.

Kamu bisa menggunakan beberapa aplikasi penyimpan password jika memang takut ada salah satu kata sandi yang terlupa.

3. Lapor ke Pihak E-Commerce

Selanjutnya adalah melaporkan ke pihak perusahaan sebagai penanggung jawab.

Hal ini mungkin bisa digunakan saat akun e-commerce milikmu tidak bisa diakses atau log in.

Meskipun belum pasti bahwa akunmu diretas, namun untuk melakukan tindakan yang tepat, sepertinya menyerahkan masalah ke pihak e-commerce adalah langkah yang baik.

4. Aktifkan Two-Factor Authentication

Sebenarnya untuk two-factor authentication ini sudah secara otomatis akan aktif di beberapa aplikasi e-commerce.

Namun, kamu harus menggunakan aplikasi tambahan yaitu Google Authenticator yang bisa kamu download di Google Play Store ataupun AppStore.

Jadi nantinya kamu diharuskan untuk scan barcode yang ditampilkan oleh aplikasi e-commerce di layar smartphone.

5. Tidak Menyimpan Akun Pembayaran

Beberapa pengguna kerap kali melakukan hal ini dengan tujuan untuk mempercepat proses pembayaran.

Namun hal tersebut sebaiknya dihindari karena kamu bisa saja mengalami peretasan dari hacker.

Selain itu, jangan isi saldo seperti OVO, Shopeepay, atau lainnya secara berlebihan.

DAFTAR PUSTAKA

Nengsih Warnia. 2019 : Implementasi Data Mining

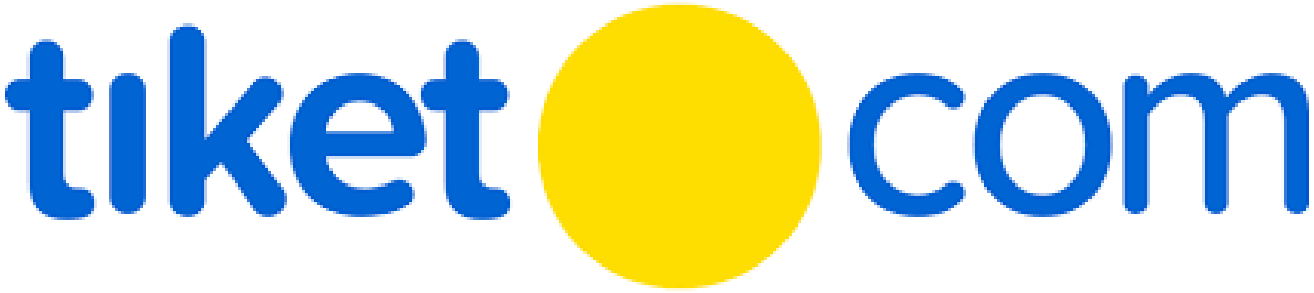
Pane, Syafrial Fachri. 2020 : Big data classification behavior menggunakan python

https://en.m.wikipedia.org/wiki/Unstructured_data

https://id.quora.com/Apa-perbedaan-antara-data-terstruktur-dan-tidak-terstruktur

Pmbobolan data pada Tiket.com

Andriansyah


tiket com

- Pada 11 November 2016, Bareskrim Polri menerima laporan pengaduan dari PT Global Network (tiket.com) tentang kasus *hacking/illegal access* atas penggunaan aplikasi jual-beli tiket *online* milik PT Global Network (tiket.com) pada sistem aplikasi jual-beli tiket *online* PT Citilink Indonesia. Pelaku melakukan *hacking/illegal access* pada server PT Citilink Indonesia (www.citilink.co.id) dari akun milik PT Global Network (tiket.com) sejak tanggal 11 sampai dengan 27 Oktober 2016.

- Kasus *illegal access* ini membuat pihak tiket.com mengalami kerugian sebesar Rp 4.124.000.982. Dan setelah diketahui oleh pihak PT Global Network (tiket.com), tiket yang belum terbang dilakukan pembatalan dan dilakukan *refund* sehingga kerugian yang dialami PT Global Network (tiket.com) sebesar Rp 1.973.784.434.

- Dari kasus yang terjadi salah satu hacker Indonesia telah memiliki akun yaitu username dan password untuk dapat masuk kedalam server milik tiket.com yang didapat dengan cara diretas. Beberapa hecker lain bertugas melakukan input data permintaan tiket pesawat dari pemberli ke aplikasi jual beli tiket online yang sudahdibuka. Setelah kode booking pesawat dibuka maka akan dikrimkan ke pembeli.

KASUS DATA BRACH
PADA TOKOPEDIA DI AWAL MEI 2020

DISUSUN OLEH :

AL-ADRI NOFA GUSANDI (192420053)

ARFA FAUZIAH (192420055)

ELPINA SARI (192420050)

Latar Belakang

- Perkembangan dunia teknologi saat ini sangat cepat, sehingga manusia dituntut untuk mengikuti perkembangan. Untuk itu dibutuhkan sumber daya manusia dalam bidang IT yang memiliki kemampuan beradaptasi secara cepat. Dalam dunia teknologi informasi saat ini kebutuhan terhadap data adalah sebuah kunci yang wajib dimiliki pada setiap lini bisnis.
- Besarnya data yang tersimpan di dalam sebuah perusahaan berkembang sangat cepat tiap harinya. Kemampuan untuk mengakses dan menganalisa data tersebut dalam pembuatan keputusan yang cepat dan cerdas menjadi kunci kesuksesan sebuah perusahaan. Data tersebut disimpan dalam lokasi, sistem, format dan skema yang berbeda dan memberikan tantangan dalam penggunaan maupun integrasinya
- Sepanjang tahun 2020, muncul rentetan kasus kebocoran data baik yang dialami pemerintah maupun perusahaan swasta seperti platform e-commerce. Kasus kebocoran data ini terjadi mulai bulan Mei 2020. Dalam kasus kebocoran tersebut, peretas mencuri data pengguna lalu menjualnya ke forum gelap.
- Pada tugas ini penulis akan membahas tentang apa penyebab kebocoran data pada situs Toko Pedia tersebut dan bagaimana cara melakukan pencegahannya

PEMBAHASAN

- **Data Breach**

Menurut Wikipedia.org (2021), Pelanggaran data adalah pelepasan informasi aman atau pribadi / rahasia yang disengaja atau tidak disengaja ke lingkungan yang tidak tepercaya. Istilah lain untuk fenomena ini antara lain keterbukaan informasi yang tidak disengaja, kebocoran data, kebocoran informasi dan juga tumpahan data. Insiden berkisar dari serangan bersama oleh topi hitam, atau individu yang meretas untuk keuntungan pribadi, terkait dengan kejahatan terorganisir, aktivis politik atau pemerintah nasional hingga pembuangan peralatan komputer bekas atau media penyimpanan data secara sembarangan dan sumber yang tidak dapat diretas.

Penyebab Kebocoran Data Pada Toko Pedia

- Awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan.
- Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020.
- Kendati membenarkan adanya upaya pencurian, Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun.

Cara Pencegahan pembobolan akun e-commers

- Dikabarkan bahwa data dari 91 juta pengguna Tokopedia telah berhasil diambil dan dijual di dark web seharga 76 juta Rupiah.
- Menteri Komunikasi dan Informatika (Menkominfo), Johnny G. Plate juga sudah memberikan tanggapan terkait masalah ini.
- Menteri Johnny mengatakan bahwa Kemenkominfo akan secara serius melakukan evaluasi, penyelidikan, dan mitigasi teknis.
- Pihak kementerian terkait juga melakukan kerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk menangani kebocoran data e-commerce ini.
- Namun, sebagai pengguna, tentunya kita juga harus melakukan beberapa antisipasi sebelum pihak berwenang yang melakukannya.
- Nextren telah memiliki beberapa cara yang mungkin bisa menjadi tindakan pencegahannya.

Berikut langkah-langkah yang kamu bisa lakukan :

1. **Aktifkan Update Otomatis**
2. **Ubah Password**
3. **Lapor ke Pihak E-Commerce**
4. **Aktifkan Two-Factor Authentication**
5. **Tidak Menyimpan Akun Pembayaran**

DAFTAR PUSTAKA

Nengsih Warnia. 2019 : Implementasi Data Mining

Pane, Syafrial Fachri. 2020 : Big data classification behavior menggunakan python

https://en.m.wikipedia.org/wiki/Unstructured_data

https://id.quora.com/Apa-perbedaan-antara-data-terstruktur-dan-tidak-terstruktur

KASUS DATA BRACH

PADA TOKO PEDIA DI AWAL MEI 2020

OLEH :

ALADRI NOFA GUSANDI

ARPA PAUZIAH

ELPINA SARI

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

2020/2021

1. Pendahuluan

Perkembangan dunia teknologi saat ini sangat cepat, sehingga manusia dituntut untuk mengikuti perkembangan. Untuk itu dibutuhkan sumber daya manusia dalam bidang IT yang memiliki kemampuan beradaptasi secara cepat. Dalam dunia teknologi informasi saat ini kebutuhan terhadap data adalah sebuah kunci yang wajib dimiliki pada setiap lini bisnis. Meskipun bisnisnya bahkan tidak berhubungan dengan dunia teknologi, namun data sangat diperlukan dalam melakukan analisis yang nantinya akan digunakan untuk pengambilan keputusan.

Besarnya data yang tersimpan di dalam sebuah perusahaan berkembang sangat cepat tiap harinya. Kemampuan untuk mengakses dan menganalisa data tersebut dalam pembuatan keputusan yang cepat dan cerdas menjadi kunci kesuksesan sebuah perusahaan. Banyak perusahaan yang terus berkembang seiring dengan berputarnya waktu, sehingga menghasilkan informasi yang heterogen dari data yang terdistribusi di berbagai sumber. Data tersebut disimpan dalam lokasi, sistem, format dan skema yang berbeda dan memberikan tantangan dalam penggunaan maupun integrasinya.

Sepanjang tahun 2020, muncul rentetan kasus kebocoran data baik yang dialami pemerintah maupun perusahaan swasta seperti platform e-commerce. Kasus kebocoran data ini terjadi mulai bulan Mei 2020. Dalam kasus kebocoran tersebut, peretas mencuri data pengguna lalu menjualnya ke forum gelap.

Pada tugas ini penulis akan membahas tentang apa penyebab kebocoran data pada situs Toko Pedia tersebut dan bagaimana cara melakukan pencegahannya.

2. PEMBAHASAN

1. Data Breach

Menurut Wikipedia.org (2021), Pelanggaran data adalah pelepasan informasi aman atau pribadi / rahasia yang disengaja atau tidak disengaja ke lingkungan yang tidak tepercaya. Istilah lain untuk fenomena ini antara lain keterbukaan informasi yang tidak disengaja, kebocoran data, kebocoran informasi dan juga tumpahan data. Insiden berkisar dari serangan bersama oleh topi hitam, atau individu yang meretas untuk keuntungan pribadi, terkait dengan kejahatan terorganisir, aktivis politik atau pemerintah nasional hingga pembuangan peralatan komputer bekas atau media penyimpanan data secara sembarangan dan sumber yang tidak dapat diretas.

2. Penyebab Kebocoran Data Pada Toko Pedia

Awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan.

Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020.

Kendati membenarkan adanya upaya pencurian, Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun.

3. Cara Pencegahan pembobolan akun e-commers

Dikabarkan bahwa data dari 91 juta pengguna Tokopedia telah berhasil diambil dan dijual di dark web seharga 76 juta Rupiah.

Menteri Komunikasi dan Informatika (Menkominfo), Johnny G. Plate juga sudah memberikan tanggapan terkait masalah ini.

Menteri Johnny mengatakan bahwa Kemenkominfo akan secara serius melakukan evaluasi, penyelidikan, dan mitigasi teknis.

Pihak kementerian terkait juga melakukan kerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk menangani kebocoran data e-commerce ini.

Namun, sebagai pengguna, tentunya kita juga harus melakukan beberapa antisipasi sebelum pihak berwenang yang melakukannya.

Nextren telah memiliki beberapa cara yang mungkin bisa menjadi tindakan pencegahannya.

Berikut langkah-langkah yang kamu bisa lakukan!

1. Aktifkan Update Otomatis

Langkah pertama yang bisa kamu lakukan adalah pengaktifan update secara otomatis pada aplikasi.

Hal ini menjadi alternatif pertama karena kamu bisa dengan cepat mendapatkan versi terbaru dari aplikasi.

Pembaruan aplikasi biasanya tidak hanya dari segi fitur, namun juga dari sisi keamanannya.

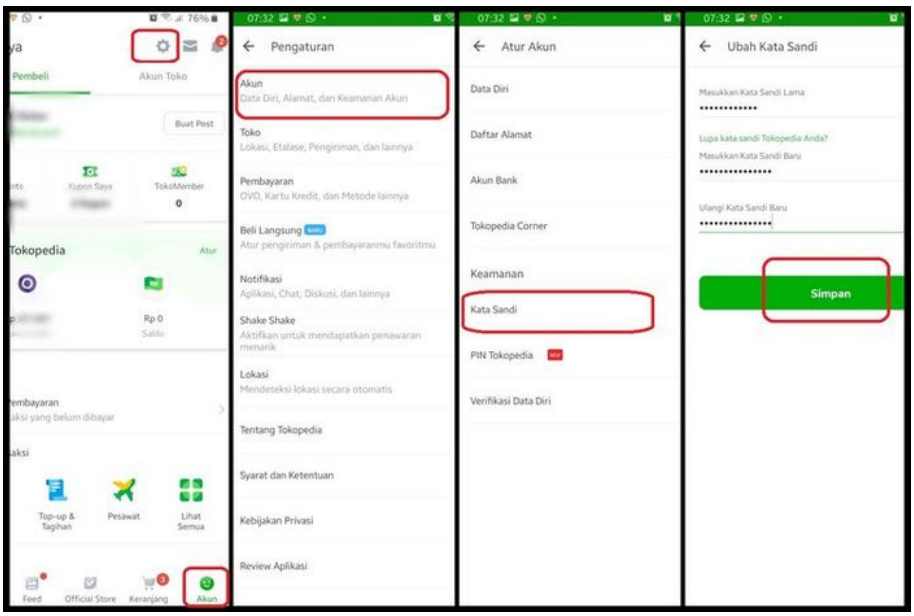
Untuk itu, cara ini Nextren anggap perlu untuk dilakukan oleh para pengguna e-commerce.

2. Ubah Password

Cara kedua yang bisa kalian gunakan untuk mengamankan data kalian adalah mengubah password.

Langkah ini memang cukup klasik, namun mengubah password dapat membuat data kamu bisa lebih aman dari para hacker.

Pihak Tokopedia sebagai perusahaan yang mengalami serangan hacker juga sempat menyarankan kepada penggunanya untuk mengganti password.



Jangan lupa juga membuat password yang unik dari setiap akun yang memasukkan data pribadimu.

Kamu bisa menggunakan beberapa aplikasi penyimpan password jika memang takut ada salah satu kata sandi yang terlupa.

3. Lapor ke Pihak E-Commerce

Selanjutnya adalah melaporkan ke pihak perusahaan sebagai penanggung jawab.

Hal ini mungkin bisa digunakan saat akun e-commerce milikmu tidak bisa diakses atau log in.

Meskipun belum pasti bahwa akunmu diretas, namun untuk melakukan tindakan yang tepat, sepertinya menyerahkan masalah ke pihak e-commerce adalah langkah yang baik.

4. Aktifkan Two-Factor Authentication

Sebenarnya untuk two-factor authentication ini sudah secara otomatis akan aktif di beberapa aplikasi e-commerce.

Namun, kamu harus menggunakan aplikasi tambahan yaitu Google Authenticator yang bisa kamu download di Google Play Store ataupun AppStore.

Jadi nantinya kamu diharuskan untuk scan barcode yang ditampilkan oleh aplikasi e-commerce di layar smartphone.

5. Tidak Menyimpan Akun Pembayaran

Beberapa pengguna kerap kali melakukan hal ini dengan tujuan untuk mempercepat proses pembayaran.

Namun hal tersebut sebaiknya dihindari karena kamu bisa saja mengalami peretasan dari hacker.

Selain itu, jangan isi saldo seperti OVO, Shopeepay, atau lainnya secara berlebihan.

DAFTAR PUSTAKA

Nengsih Warnia. 2019 : Implementasi Data Mining

Pane, Syafrial Fachri. 2020 : Big data classification behavior menggunakan python

https://en.m.wikipedia.org/wiki/Unstructured_data

https://id.quora.com/Apa-perbedaan-antara-data-terstruktur-dan-tidak-terstruktur

KASUS DATA BRACH
PADA TOKOPEDIA DI AWAL MEI 2020

DISUSUN OLEH :

ELPINA SARI (192420050)

ARFA FAUZIAH (192420055)

AL-ADRI NOFA GUSANDI (192420053)

Latar Belakang

- Perkembangan dunia teknologi saat ini sangat cepat, sehingga manusia dituntut untuk mengikuti perkembangan. Untuk itu dibutuhkan sumber daya manusia dalam bidang IT yang memiliki kemampuan beradaptasi secara cepat. Dalam dunia teknologi informasi saat ini kebutuhan terhadap data adalah sebuah kunci yang wajib dimiliki pada setiap lini bisnis.
- Besarnya data yang tersimpan di dalam sebuah perusahaan berkembang sangat cepat tiap harinya. Kemampuan untuk mengakses dan menganalisa data tersebut dalam pembuatan keputusan yang cepat dan cerdas menjadi kunci kesuksesan sebuah perusahaan. Data tersebut disimpan dalam lokasi, sistem, format dan skema yang berbeda dan memberikan tantangan dalam penggunaan maupun integrasinya
- Sepanjang tahun 2020, muncul rentetan kasus kebocoran data baik yang dialami pemerintah maupun perusahaan swasta seperti platform e-commerce. Kasus kebocoran data ini terjadi mulai bulan Mei 2020. Dalam kasus kebocoran tersebut, peretas mencuri data pengguna lalu menjualnya ke forum gelap.
- Pada tugas ini penulis akan membahas tentang apa penyebab kebocoran data pada situs Toko Pedia tersebut dan bagaimana cara melakukan pencegahannya

PEMBAHASAN

- **Data Breach**

Menurut Wikipedia.org (2021), Pelanggaran data adalah pelepasan informasi aman atau pribadi / rahasia yang disengaja atau tidak disengaja ke lingkungan yang tidak tepercaya. Istilah lain untuk fenomena ini antara lain keterbukaan informasi yang tidak disengaja, kebocoran data, kebocoran informasi dan juga tumpahan data. Insiden berkisar dari serangan bersama oleh topi hitam, atau individu yang meretas untuk keuntungan pribadi, terkait dengan kejahatan terorganisir, aktivis politik atau pemerintah nasional hingga pembuangan peralatan komputer bekas atau media penyimpanan data secara sembarangan dan sumber yang tidak dapat diretas.

Penyebab Kebocoran Data Pada Toko Pedia

- Awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan.
- Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020.
- Kendati membenarkan adanya upaya pencurian, Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun.

Cara Pencegahan pembobolan akun e-commers

- Dikabarkan bahwa data dari 91 juta pengguna Tokopedia telah berhasil diambil dan dijual di dark web seharga 76 juta Rupiah.
- Menteri Komunikasi dan Informatika (Menkominfo), Johnny G. Plate juga sudah memberikan tanggapan terkait masalah ini.
- Menteri Johnny mengatakan bahwa Kemenkominfo akan secara serius melakukan evaluasi, penyelidikan, dan mitigasi teknis.
- Pihak kementerian terkait juga melakukan kerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk menangani kebocoran data e-commerce ini.
- Namun, sebagai pengguna, tentunya kita juga harus melakukan beberapa antisipasi sebelum pihak berwenang yang melakukannya.
- Nextren telah memiliki beberapa cara yang mungkin bisa menjadi tindakan pencegahannya.

Berikut langkah-langkah yang kamu bisa lakukan :

1. **Aktifkan Update Otomatis**
2. **Ubah Password**
3. **Lapor ke Pihak E-Commerce**
4. **Aktifkan Two-Factor Authentication**
5. **Tidak Menyimpan Akun Pembayaran**

DAFTAR PUSTAKA

Nengsih Warnia. 2019 : Implementasi Data Mining

Pane, Syafrial Fachri. 2020 : Big data classification behavior menggunakan python

https://en.m.wikipedia.org/wiki/Unstructured_data

https://id.quora.com/Apa-perbedaan-antara-data-terstruktur-dan-tidak-terstruktur

KASUS DATA BRACH

PADA TOKO PEDIA DI AWAL MEI 2020

OLEH :

ALADRI NOFA GUSANDI

ARPA PAUZIAH

ELPINA SARI

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

2020/2021

1. Pendahuluan

Perkembangan dunia teknologi saat ini sangat cepat, sehingga manusia dituntut untuk mengikuti perkembangan. Untuk itu dibutuhkan sumber daya manusia dalam bidang IT yang memiliki kemampuan beradaptasi secara cepat. Dalam dunia teknologi informasi saat ini kebutuhan terhadap data adalah sebuah kunci yang wajib dimiliki pada setiap lini bisnis. Meskipun bisnisnya bahkan tidak berhubungan dengan dunia teknologi, namun data sangat diperlukan dalam melakukan analisis yang nantinya akan digunakan untuk pengambilan keputusan.

Besarnya data yang tersimpan di dalam sebuah perusahaan berkembang sangat cepat tiap harinya. Kemampuan untuk mengakses dan menganalisa data tersebut dalam pembuatan keputusan yang cepat dan cerdas menjadi kunci kesuksesan sebuah perusahaan. Banyak perusahaan yang terus berkembang seiring dengan berputarnya waktu, sehingga menghasilkan informasi yang heterogen dari data yang terdistribusi di berbagai sumber. Data tersebut disimpan dalam lokasi, sistem, format dan skema yang berbeda dan memberikan tantangan dalam penggunaan maupun integrasinya.

Sepanjang tahun 2020, muncul rentetan kasus kebocoran data baik yang dialami pemerintah maupun perusahaan swasta seperti platform e-commerce. Kasus kebocoran data ini terjadi mulai bulan Mei 2020. Dalam kasus kebocoran tersebut, peretas mencuri data pengguna lalu menjualnya ke forum gelap.

Pada tugas ini penulis akan membahas tentang apa penyebab kebocoran data pada situs Toko Pedia tersebut dan bagaimana cara melakukan pencegahannya.

2. PEMBAHASAN

1. Data Breach

Menurut Wikipedia.org (2021), Pelanggaran data adalah pelepasan informasi aman atau pribadi / rahasia yang disengaja atau tidak disengaja ke lingkungan yang tidak tepercaya. Istilah lain untuk fenomena ini antara lain keterbukaan informasi yang tidak disengaja, kebocoran data, kebocoran informasi dan juga tumpahan data. Insiden berkisar dari serangan bersama oleh topi hitam, atau individu yang meretas untuk keuntungan pribadi, terkait dengan kejahatan terorganisir, aktivis politik atau pemerintah nasional hingga pembuangan peralatan komputer bekas atau media penyimpanan data secara sembarangan dan sumber yang tidak dapat diretas.

2. Penyebab Kebocoran Data Pada Toko Pedia

Awal Mei 2020, sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Kasus kebocoran data pengguna Tokopedia ini mulanya diungkap oleh akun Twitter @underthebreach, yang kerap membagikan isu soal peretasan.

Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password. Data tersebut kabarnya sudah dikumpulkan peretas sejak Maret 2020.

Kendati membenarkan adanya upaya pencurian, Tokopedia mengklaim bahwa informasi milik pengguna tetap aman dan terlindungi. VP of Corporate Communications Tokopedia, Nuraini Razak mengatakan bahwa password milik pengguna telah terlindungi dan dienkripsi. Tokopedia juga menerapkan sistem kode OTP (one-time password) yang hanya bisa diakses secara real time oleh pemilik akun.

3. Cara Pencegahan pembobolan akun e-commers

Dikabarkan bahwa data dari 91 juta pengguna Tokopedia telah berhasil diambil dan dijual di dark web seharga 76 juta Rupiah.

Menteri Komunikasi dan Informatika (Menkominfo), Johnny G. Plate juga sudah memberikan tanggapan terkait masalah ini.

Menteri Johnny mengatakan bahwa Kemenkominfo akan secara serius melakukan evaluasi, penyelidikan, dan mitigasi teknis.

Pihak kementerian terkait juga melakukan kerja sama dengan Badan Siber dan Sandi Negara (BSSN) untuk menangani kebocoran data e-commerce ini.

Namun, sebagai pengguna, tentunya kita juga harus melakukan beberapa antisipasi sebelum pihak berwenang yang melakukannya.

Nextren telah memiliki beberapa cara yang mungkin bisa menjadi tindakan pencegahannya.

Berikut langkah-langkah yang kamu bisa lakukan!

1. Aktifkan Update Otomatis

Langkah pertama yang bisa kamu lakukan adalah pengaktifan update secara otomatis pada aplikasi.

Hal ini menjadi alternatif pertama karena kamu bisa dengan cepat mendapatkan versi terbaru dari aplikasi.

Pembaruan aplikasi biasanya tidak hanya dari segi fitur, namun juga dari sisi keamanannya.

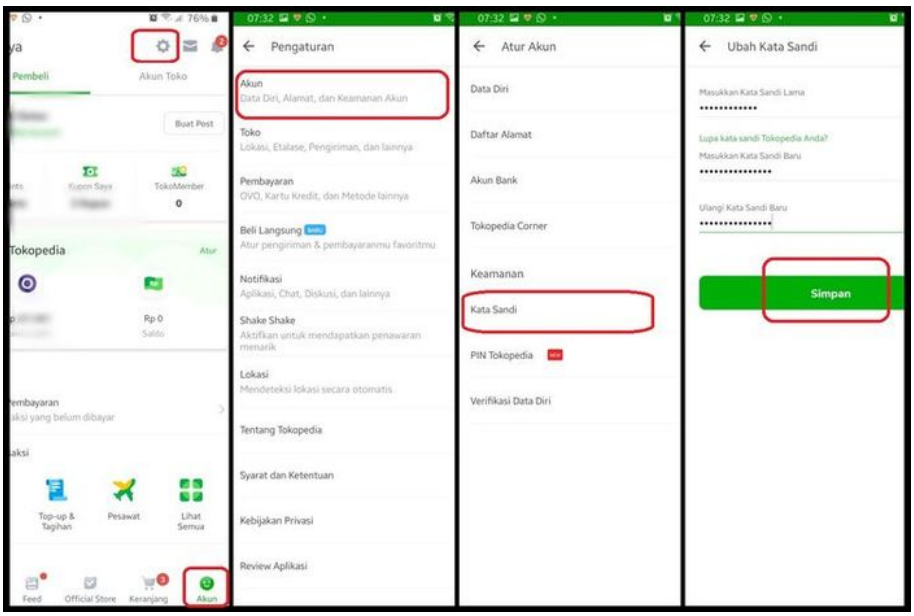
Untuk itu, cara ini Nextren anggap perlu untuk dilakukan oleh para pengguna e-commerce.

2. Ubah Password

Cara kedua yang bisa kalian gunakan untuk mengamankan data kalian adalah mengubah password.

Langkah ini memang cukup klasik, namun mengubah password dapat membuat data kamu bisa lebih aman dari para hacker.

Pihak Tokopedia sebagai perusahaan yang mengalami serangan hacker juga sempat menyarankan kepada penggunanya untuk mengganti password.



Jangan lupa juga membuat password yang unik dari setiap akun yang memasukkan data pribadimu.

Kamu bisa menggunakan beberapa aplikasi penyimpan password jika memang takut ada salah satu kata sandi yang terlupa.

3. Lapor ke Pihak E-Commerce

Selanjutnya adalah melaporkan ke pihak perusahaan sebagai penanggung jawab.

Hal ini mungkin bisa digunakan saat akun e-commerce milikmu tidak bisa diakses atau log in.

Meskipun belum pasti bahwa akunmu diretas, namun untuk melakukan tindakan yang tepat, sepertinya menyerahkan masalah ke pihak e-commerce adalah langkah yang baik.

4. Aktifkan Two-Factor Authentication

Sebenarnya untuk two-factor authentication ini sudah secara otomatis akan aktif di beberapa aplikasi e-commerce.

Namun, kamu harus menggunakan aplikasi tambahan yaitu Google Authenticator yang bisa kamu download di Google Play Store ataupun AppStore.

Jadi nantinya kamu diharuskan untuk scan barcode yang ditampilkan oleh aplikasi e-commerce di layar smartphone.

5. Tidak Menyimpan Akun Pembayaran

Beberapa pengguna kerap kali melakukan hal ini dengan tujuan untuk mempercepat proses pembayaran.

Namun hal tersebut sebaiknya dihindari karena kamu bisa saja mengalami peretasan dari hacker.

Selain itu, jangan isi saldo seperti OVO, Shopeepay, atau lainnya secara berlebihan.

DAFTAR PUSTAKA

Nengsih Warnia. 2019 : Implementasi Data Mining

Pane, Syafrial Fachri. 2020 : Big data classification behavior menggunakan python

https://en.m.wikipedia.org/wiki/Unstructured_data

https://id.quora.com/Apa-perbedaan-antara-data-terstruktur-dan-tidak-terstruktur

ANALISIS KASUS *DATA BREACH* ILHAM BINTANG

Dosen Pengasuh :

Dr. Widya Cholil, S.Kom., M.IT.

Disusun Oleh :

1. M. Iqbal Rivana (192420057)
2. Isti Ma'atun Nasichah (192420051)
3. Fadel M. Madjid (192420052)

PROGRAM STUDI TEKNIK INFORMATIKA – S2

PROGRAM PASCASARJANA

UNIVERSITAS BINA DARMA

PALEMBANG

KRONOLOGI KEJADIAN

Ilham Bintang, lahir di Makassar, 10 Mei 1955, merupakan seorang wartawan dan pengusaha Indonesia yang dikenal sebagai "pelopor jurnalistik infotainment" di Indonesia dan memiliki 15 slot acara usaha hiburan televisi di stasiun televisi swasta. Saat ini, Ilham Bintang adalah Sekretaris Dewan Kehormatan Persatuan Wartawan Indonesia (PWI) Pusat dan Pemimpin Redaksi Tabloid Cek & Ricek (C&R).

Pada awal tahun 2020 kemarin, wartawan senior Ilham Bintang menjadi pemberitaan banyak media. Penyebabnya adalah insiden penyalahgunaan *simcard* miliknya yang digunakan oleh orang lain saat Ilham Bintang sedang berada di Australia. Pencurian identitas pribadi tersebut berujung pada pembobolan rekening milik Ilham Bintang di Bank Commonwealth yang mengakibatkan hilangnya uang ratusan juta rupiah. Kronologi kasus pembobolan rekening bank Ilham Bintang adalah sebagai berikut:

1. Bermula dari kehilangan sinyal

Dalam sidang, Ilham bintang menceritakan bagaimana ia menyadari bahwa rekeningnya telah dibobol. Semua bermula saat ia sedang berada di Sydney Airport, Australia pada tanggal 4 Januari 2020, di ponsel muncul jaringan SOS, padahal, ia sudah mengaktifkan paket roaming Indosat sebelum berangkat ke Australia. Selang beberapa hari kemudian, tepatnya 6 Januari 2020, jaringan di ponsel Ilham masih menunjukan sinyal SOS. Ilham yang butuh melakukan transaksi perbankan kemudian mengkoneksikan sinyal ponselnya dengan jaringan wifi. Namun, saat itu ia tidak bisa mengakses aplikasi M-Banking dari Bank Commonwelth yang biasa ia gunakan. Ilham memutuskan mendatangi bank Commonwealth yang ada di Melbourne untuk mengkonfirmasi apa yang sedang terjadi. Ternyata uang sebesar 25.000 dollar Australia atau setara 250 juta rupiah telah raib. Kemudian, ia menghubungi agensinya yang berada di Jakarta. Ia meminta agensinya tersebut mengecek uangnya di bank yang sama, namun berbentuk rupiah. Hasilnya pun serupa. Uang sebesar 16 juta rupiah juga telah hilang. Selain itu, terdapat transaksi sebesar 120 juta rupiah di tiga kartu kredit Ilham, yaitu BNI, BCA dan Citibank.

2. Melapor ke Kepolisian Melbourne - Australia

Langkah pertama yang dilakukan Ilham saat itu adalah melapor ke Kepolisian Melbourne karena mengira itu adalah kejahatan internasional karena saat itu uang dalam bentuk dollar Australia. Kemudian Ilham pulang ke Indonesia dan ternyat, sinyal *simcard*-nya masih menghilang. Ia kemudian mendatangi gerai Indosat dan mengetahui bahwa seseorang telah mengambil alih *simcard*-nya. Seseorang yang mengaku sebagai Ilham Bintang mengurus kehilangan nomor ponsel di gerai Indosat di kawasan Bintaro. Setelah mendapatkan *simcard* itu, barulah mereka bisa mengakses berbagai rekening bank tersebut. Ilham kemudian melaporkan hal tersebut ke kepolisian setempat hingga akhirnya komplotan pelaku ditangkap.

Peran para tersangka :

a. Tersangka D, di tangkap di palembang. D berperan sebagai bos dari sindikat ini. Dia membeli data-data nasabah bank dan slip OJK untuk mengetahui data-data korban sebagai targetnya. D bertugas memastikan ponsel Ilham Bintang tetap dalam kondisi mati agar para pelaku bisa membuat SIM card dengan data korban.

b. Tersangka H, pegawai Bank, H yang menjual data-data korban. Tersangka H punya akses bisa mendapat slip OJK. Di situ ada data-data pribadi lengkap seseorang yang memiliki rekening atau limit rekening.

c. Tersangka R dan HN yang berperan membantu H untuk menyiapkan data-data yang dijual.

d. Tersangka W, AY dan TR yang berada di Jakarta untuk menduplikat *simcard* korban dengan cara datang langsung ke gerai Indosat di Jakarta Barat.

e. Tersangka JW yang membuat KTP palsu dari Ilham Bintang dengan foto yang tertera foto orang lain

Dari *simcard* tersebut, D mulai menelisik email hingga akun m-banking milik Ilham. D mulai masuk ke aplikasi *Yahoo* untuk mengetahui email Ilham. Saat diminta me-*reset* (untuk membuka email Ilham), dikirim OTP (*One Time Password*) ke nomor telepon baru. Jadi *password* email pribadi Ilham dapat diganti. Setelah email terbuka, terbuka juga data bank, sehingga dua rekening habis terkuras.

3. Menyalahkan pihak Indosat

Dalam persidangan tersebut, Ilham sempat menyalahkan operator penyedia layanan kartu perdana Indosat karena dianggap melakukan kelalaian hingga rekeningnya berhasil dibobol. Menurut Ilham, pegawai Indosat di gerai Bintaro telah melakukan kelalaian sehingga nomor ponselnya bisa diambil alih oleh para terdakwa. Selain heran dengan waktu pengurusan penggantian *simcard* yang cepat, Ilham juga mendapat keterangan dari Indosat bahwa mereka lupa membuat salinan KTP yang digunakan para tersangka. Ia menyalahkan pihak Indosat karena dianggap tidak menjalankan penggantian nomor ponsel sesuai SOP yang seharusnya.

4. Terdakwa membantah membobol kartu kredit

Salah satu terdakwa dalam kasus tersebut membantah bahwa ia yang membobol kartu kredit BCA korban. Ia mengakui bahwa ia mengambil uang ratusan juta dari rekening Bank Commonwealth. Namun, hakim tidak terlalu mempermasalahkan hal tersebut karena pada akhirnya pihak bank berhasil membatalkan seluruh transaksi melalui kartu kredit Ilham. Kerugian yang dirasakan Ilham hanya berasal dari pembobolan di bank Commonwealth yang membuatnya kehilangan uang senilai 265 juta rupiah.

5. Hakim memberikan teguran kepada jaksa

Dalam persidangan kemarin sempat diwarnai beberapa teguran hakim kepada jaksa. Jaksa Penuntut Umum (JPU) Mudjiono ditegur karena tidak membawa barang bukti yang diperlukan serta tidak masuknya sejumlah saksi dalam persidangan tersebut. Teguran pertama dilayangkan Kamaludin ketika ia meminta barang bukti berupa surat keterangan dari pihak Indosat. Namun setelah mengecek serangkaian barang bukti yang ia pegang, Mudjiono mengaku tidak membawanya. Hakim kemudian menanyakan apakah foto copy KTP Ilham Bintang yang menjadi barang bukti di sidang terdakwa lainnya juga menjadi barang bukti dalam kasus tersebut. Namun, JPU menyebutkan bahwa foto copy KTP tersebut tidak dicantumkan. Karena kesalahan jaksa tersebut, majelis hakim terpaksa meminta Ilham Bintang untuk kembali hadir dalam persidangan selanjutnya.

Kemudian, hakim juga sempat menanyakan kepada Jaksa apakah terdakwa pembuat KTP palsu yang disidangkan terpisah menjadi saksi dalam sidang tersebut.

Setelah mengecek daftar saksi, Mudjianto menyampaikan bahwa ia tidak memasukkannya kedalam daftar saksi. Adapun dalam persidangan tersebut, terdapat lima orang terdakwa yang menjalani persidangan. Lima terdakwa itu antara lain Desar (20), Teti Rosmiawati (46), Wasno (52), Amran Yunianto (53), dan Pegik (28). Sementara tiga terdakwa lainnya yang terlibat dalam komplotan tersebut disidang secara terpisah di Pengadilan Negeri Jakarta Barat. Mereka didakwa dengan Pasal 35 juncto Pasal 51 ayat 1 juncto Pasal 30 juncto Pasal 46 ayat 1 UU RI 11 Tahun 2008 tentang ITE dan atau Pasal 363 KUHP, Pasal 263 KUHP, Pasal 3 dan 4 juncto Pasal 10 UU RI nomor 8 tahun 2010 tentang pencegahan dan pemberantasan tindak pidana pencucian uang.

KERUGIAN

Dari kejadian pembobolan rekening bank Ilham Bintang tersebut dapat mengakibatkan kerugian-kerugian yang bersifat materil maupun immateril bagi korban, antara lain sebagai berikut :

1. Kerugian materil hingga nominal 265 juta rupiah.
2. Ketidaknyamanan atas tindakan cybercrime (pencurian data pribadi) pada pihak korban sebagai pengguna.
3. Trauma atau efek psikologis pada korban.
4. Hilangnya kepercayaan terhadap sistem keamanan dan hukum di Indonesia.

Kerugian tidak hanya dialami oleh Ilham Bintang saja, namun juga dirasakan oleh pihak Indosat dan Bank Commonwealth, yaitu :

1. Hilangnya reputasi, kredibilitas, integritas dan kepercayaan dari masyarakat yang berdampak dalam waktu yang cukup lama.
2. Berdampak buruk pada lini keuangan dalam organisasi
3. Terlibat dalam kasus hukum yang rumit dan panjang serta berisiko terkena denda karena pelanggaran hukum perdata.

CARA PENANGANAN

1. Identifikasi

Berdasarkan kasus Ilham Bintang, dapat diidentifikasi 2 jenis cara bagaimana kebocoran data dapat terjadi, yaitu :

a. Keterlibatan Orang Dalam

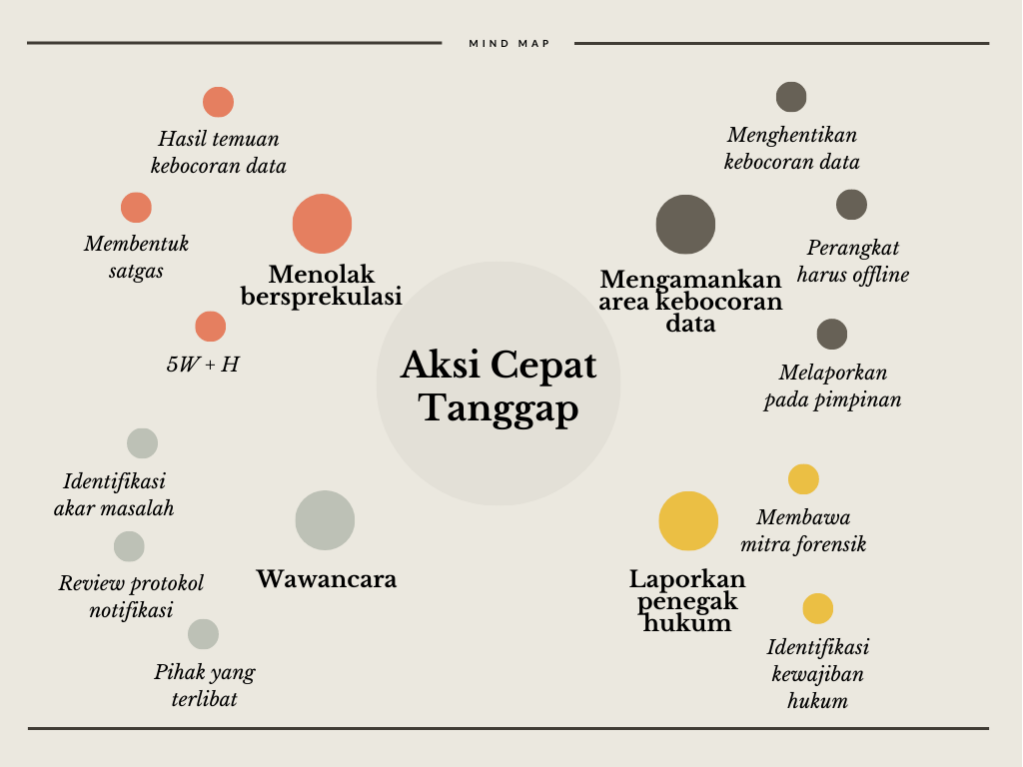
Kebocoran data disebabkan oleh karyawan sebuah institusi itu sendiri, mantan karyawan, atau oleh karyawan yang berhasil dikelabui dengan *social engineering* sehingga tanpa sadar ia memberikan data ataupun akses terhadap data.

b. Kelalaian

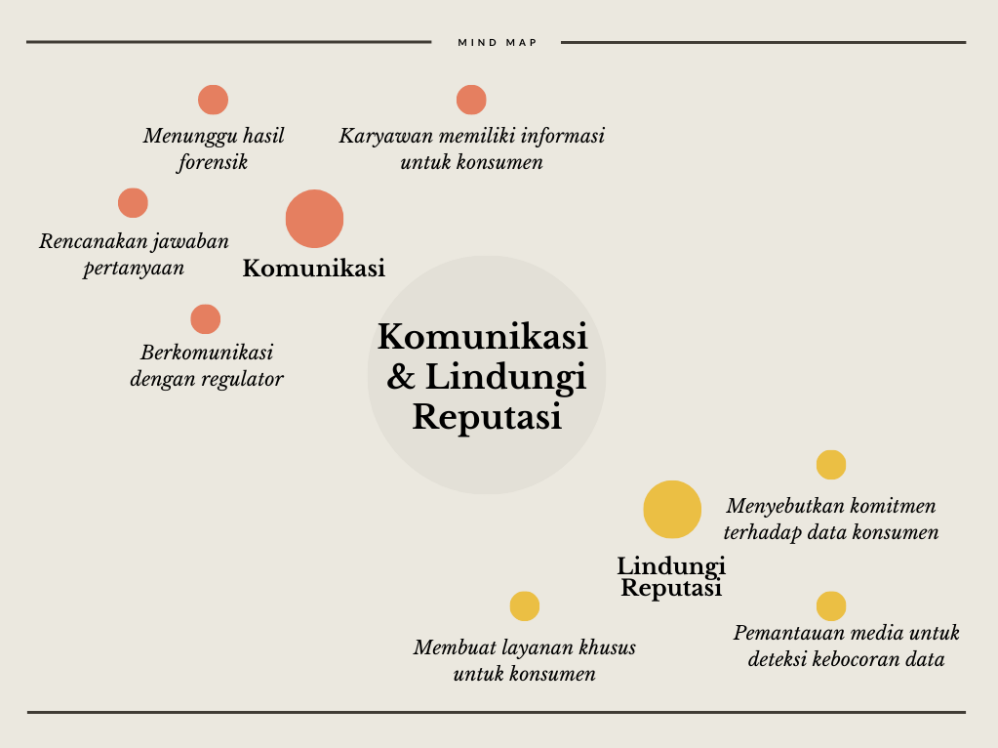
Kebocoran data disebabkan karena tidak memadainya sistem keamanan yang dimiliki. Hal ini termasuk juga tidak diterapkannya sistem atau protokol pengamanan dasar untuk pencegahan terjadinya kebocoran data.

2. Cara Penanganan (Proses Tanggap Insiden)

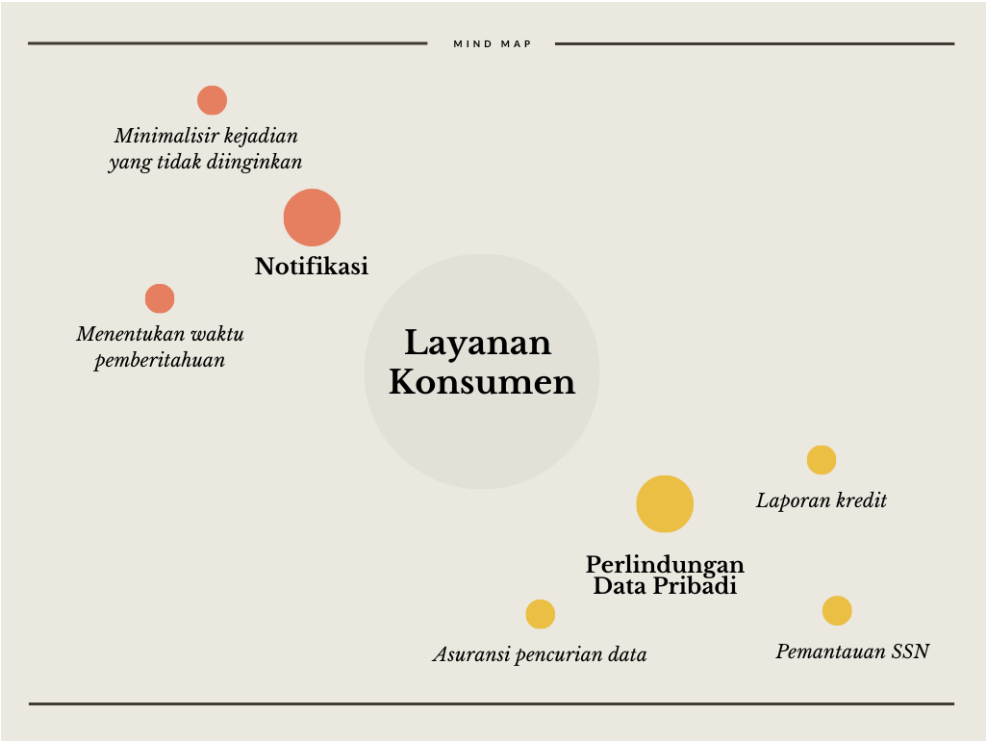
a. Aksi Cepat Tanggap



b. Komunikasi dan Lindungi Reputasi



c. Layanan Konsumen

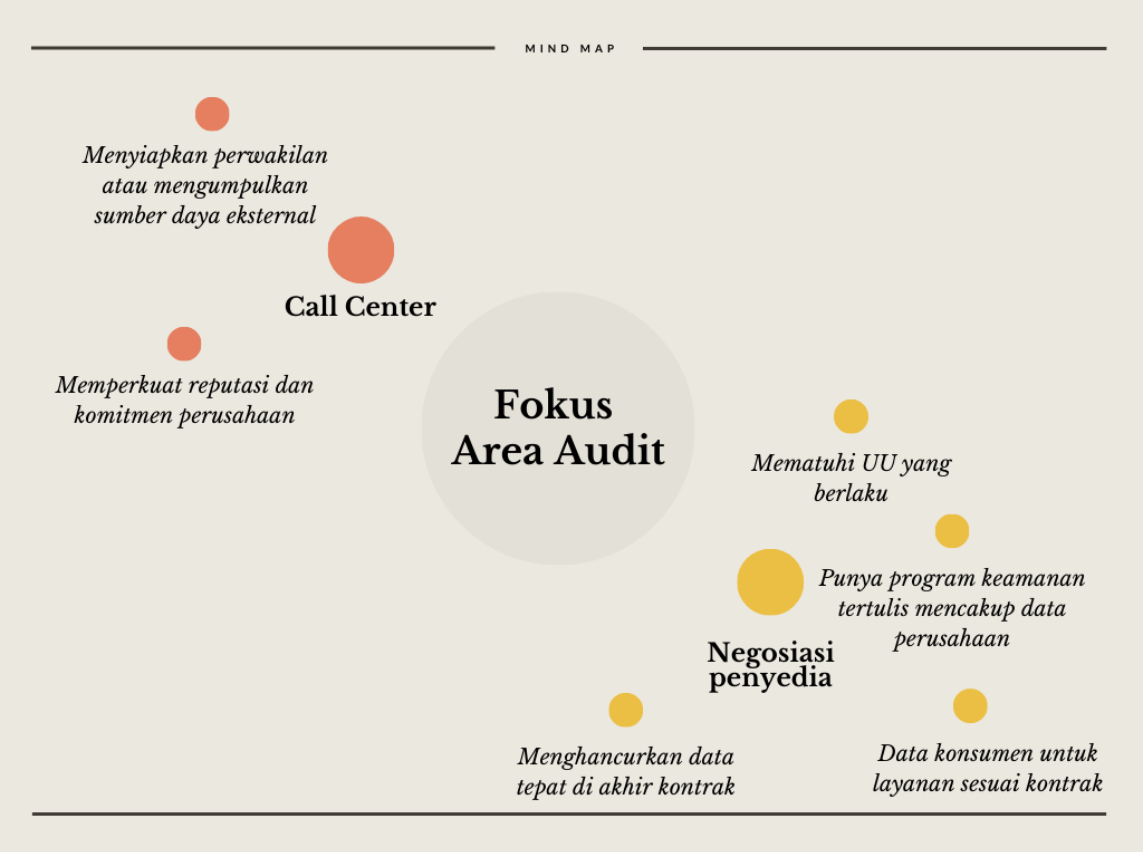


PELAKSANAAN AUDIT DATA

Setelah membuat perencanaan, perusahaan harus melakukan audit dan menguji perencanaan yang telah dibuat. Tujuannya adalah untuk membantu mengatasi permasalahan masing-masing, termasuk pelanggaran internal, serangan eksternal, berbagi data tanpa sengaja dan kehilangan/pencurian perangkat fisik. Selain itu, juga perlu untuk selalu memperbarui rencana perusahaan untuk menghindari ancaman baru yang tidak terduga yang muncul di waktu yang akan datang.

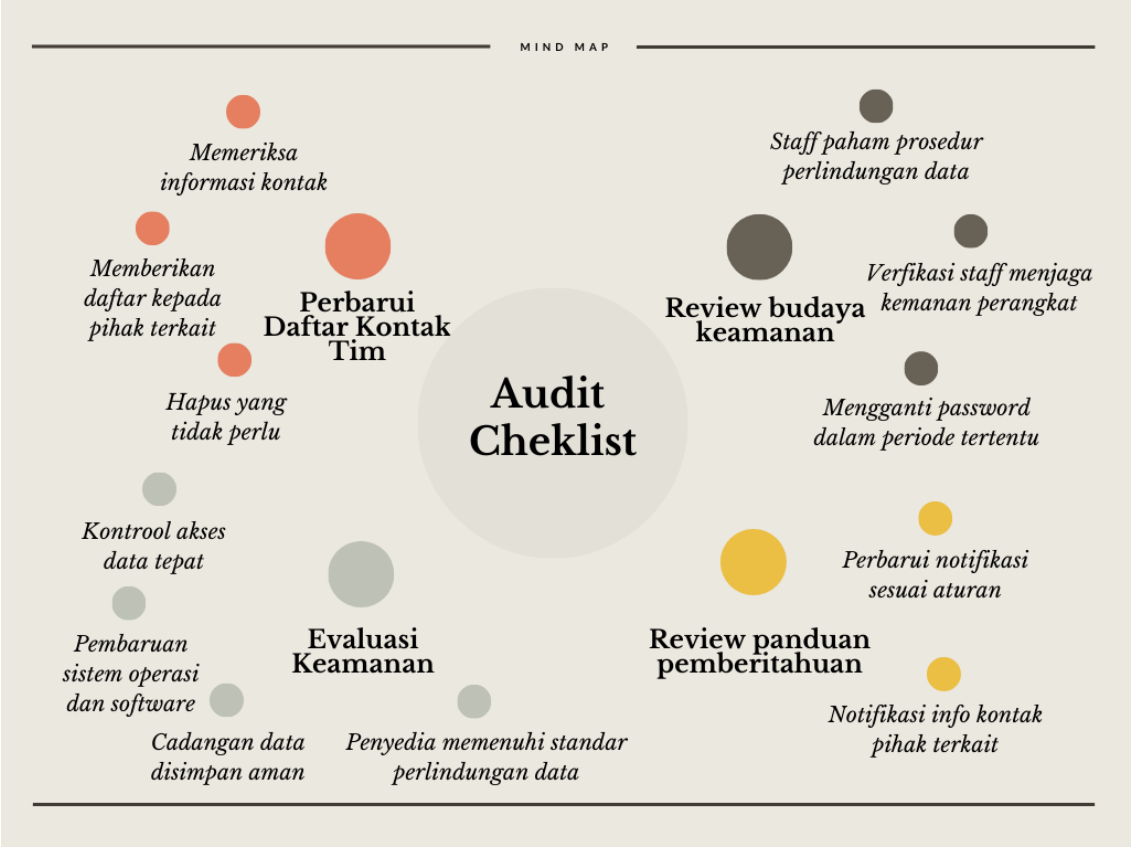
1. Fokus Area

Berikut ini adalah beberapa area yang dilaksanakan audit, yaitu :



2. Audit Checklist

Berikut ini adalah langkah yang dilakukan pada saat audit sesuai ruang lingkup respon perusahaan, yaitu :


MIND MAP
Audit Cheklist
Memeriksa informasi kontak
Memberikan daftar kepada pihak terkait
Perbarui Daftar Kontak Tim
Hapus yang tidak perlu
Kontrool akses data tepat
Pembaruan sistem operasi dan software
Evaluasi Keamanan
Cadangan data disimpan aman
Penyedia memenuhi standar perlindungan data
Staff paham prosedur perlindungan data
Review budaya keamanan
Verfikasi staff menjaga kemanan perangkat
Mengganti password dalam periode tertentu
Perbarui notifikasi sesuai aturan
Review panduan pemberitahuan
Notifikasi info kontak pihak terkait

REKOMENDASI

a. Memberikan tim Pusat Operasi Keamanan (SOC) dengan akses ke intelijen ancaman terbaru dan mendapatkan informasi terkini tentang alat, teknik serta taktik baru dan terkini yang digunakan oleh aktor ancaman dan pelaku *cyber crime*.
b. Mengimplementasikan solusi EDR untuk mendeteksi level *endpoint*, investigasi, dan remediasi insiden secara tepat waktu.
c. Selain mengadopsi perlindungan *endpoint* yang penting, juga perlu menerapkan solusi keamanan tingkat perusahaan yang mendeteksi ancaman lanjutan di tingkat jaringan pada tahap awal.
d. Menerapkan pelatihan dan kegiatan yang mengedukasi karyawan tentang dasar-dasar keamanan *cyber*, misalnya tidak membuka atau menyimpan file dari email atau situs web yang tidak dikenal karena dapat membahayakan seluruh perusahaan.
e. Secara berkala mengingatkan staf bagaimana menangani data sensitif, misalnya hanya menyimpan layanan cloud terpercaya dengan otentikasi diaktifkan, tidak membaginya kepada pihak ketiga yang tidak dipercaya.
f. Memiliki cadangan data penting dan melakukan pembaruan peralatan dan aplikasi TI secara teratur untuk menghindari kerentanan yang tidak tertandingi yang dapat menjadi alasan terjadinya pelanggaran.
g. Menggunakan produk *endpoint* khusus yang menuntut manajemen minimum yang memungkinkan karyawan untuk melakukan pekerjaan utama mereka namun tetap terlindung dari malware, ransomware, pengambilalihan akun, penipuan online, dan penipuan.

REFERENSI

[1] AllClear ID: "Data Breach Incident Response Workbook" https://dpoacademy.gr/_files/20000003-ba715bc634/ACID_Self_Service_Incident_Response_Workbook.pdf

[2] Experian: "Data Breach Response Guide" https://www.experian.com/assets/data-breach/brochures/response-guide.pdf

[3] https://id.wikipedia.org/wiki/Ilham_Bintang#:~:text=H.%20Ilham%20Bintang%20(lahir%20di,televisi%20di%20stasiun%20televisi%20swasta

[4] https://megapolitan.kompas.com/read/2020/02/05/13355011/kronologi-dan-peran-8-pelaku-pembobolan-rekening-ilham-bintang?page=all

[5] Panduan Menghadapi Data Breach, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas), Badan Siber dan Sandi Negara (BSSN)

ANALISIS KASUS *DATA BREACH* ILHAM BINTANG

oleh :

1.M. Iqbal Rivana (192420057)

2.Isti Ma'atun Nasichah (192420051)

3.Fadel M. Madjid (192420052)

OUTLINE

1. Pendahuluan
2. Kronologi Kejadian
3. Kerugian
4. Cara Penanganan
5. Audit Data
6. Rekomendasi

PENDAHULUAN

Ilham Bintang, lahir di Makassar, 10 Mei 1955, merupakan seorang wartawan dan pengusaha Indonesia yang dikenal sebagai "pelopor jurnalistik infotainment" di Indonesia. Saat ini, Ilham Bintang adalah Sekretaris Dewan Kehormatan Persatuan Wartawan Indonesia (PWI) Pusat dan Pemimpin Redaksi Tabloid Cek & Ricek (C&R).

Pada awal tahun 2020 kemarin, Ilham Bintang mengalami insiden penyalahgunaan simcard (operator Indosat) miliknya yang digunakan oleh orang lain saat Ilham Bintang berada di Australia. Pencurian identitas pribadi tersebut berujung pada pembobolan rekening milik Ilham Bintang di Bank Commonwealth yang mengakibatkan hilangnya uang ratusan juta rupiah.

KRONOLOGI KEJADIAN

Kronologi kasus pembobolan rekening bank Ilham Bintang adalah sbb:

a. Bemula dari kehilangan sinyal.
b. Melapor ke Kepolisian Melbourne - Australia.
c. Menyalahkan pihak Indosat.
d. Terdakwa membantah membobol kartu kredit.
e. Hakim memberikan teguran kepada jaksa.

KERUGIAN

Kerugian-kerugian yang bersifat materil maupun immateril bagi korban, yaitu :

a. Kerugian materil hingga nominal 265 juta rupiah.
b. Ketidaknyamanan atas tindakan cybercrime (pencurian data pribadi) pada pihak korban sebagai pengguna.
c. Trauma atau efek psikologis pada korban.
d. Hilangnya kepercayaan terhadap sistem keamanan dan hukum di Indonesia.

Kerugian yang dialami oleh pihak Indosat dan Bank Commonwealth, yaitu :

a. Hilangnya reputasi, kredibilitas, integritas dan kepercayaan dari masyarakat yang berdampak dalam waktu yang cukup lama.
b. Berdampak buruk pada lini keuangan dalam organisasi
c. Terlibat dalam kasus hukum yang rumit dan panjang serta berisiko terkena denda karena pelanggaran hukum perdata.

IDENTIFIKASI KEBOCORAN DATA

Berdasarkan kasus Ilham Bintang, dapat diidentifikasi 2 jenis cara bagaimana kebocoran data dapat terjadi, yaitu :

a. Keterlibatan Orang Dalam

Kebocoran data disebabkan oleh karyawan sebuah institusi itu sendiri, mantan karyawan, atau oleh karyawan yang berhasil dikelabui dengan *social engineering* sehingga tanpa sadar ia memberikan data ataupun akses terhadap data.

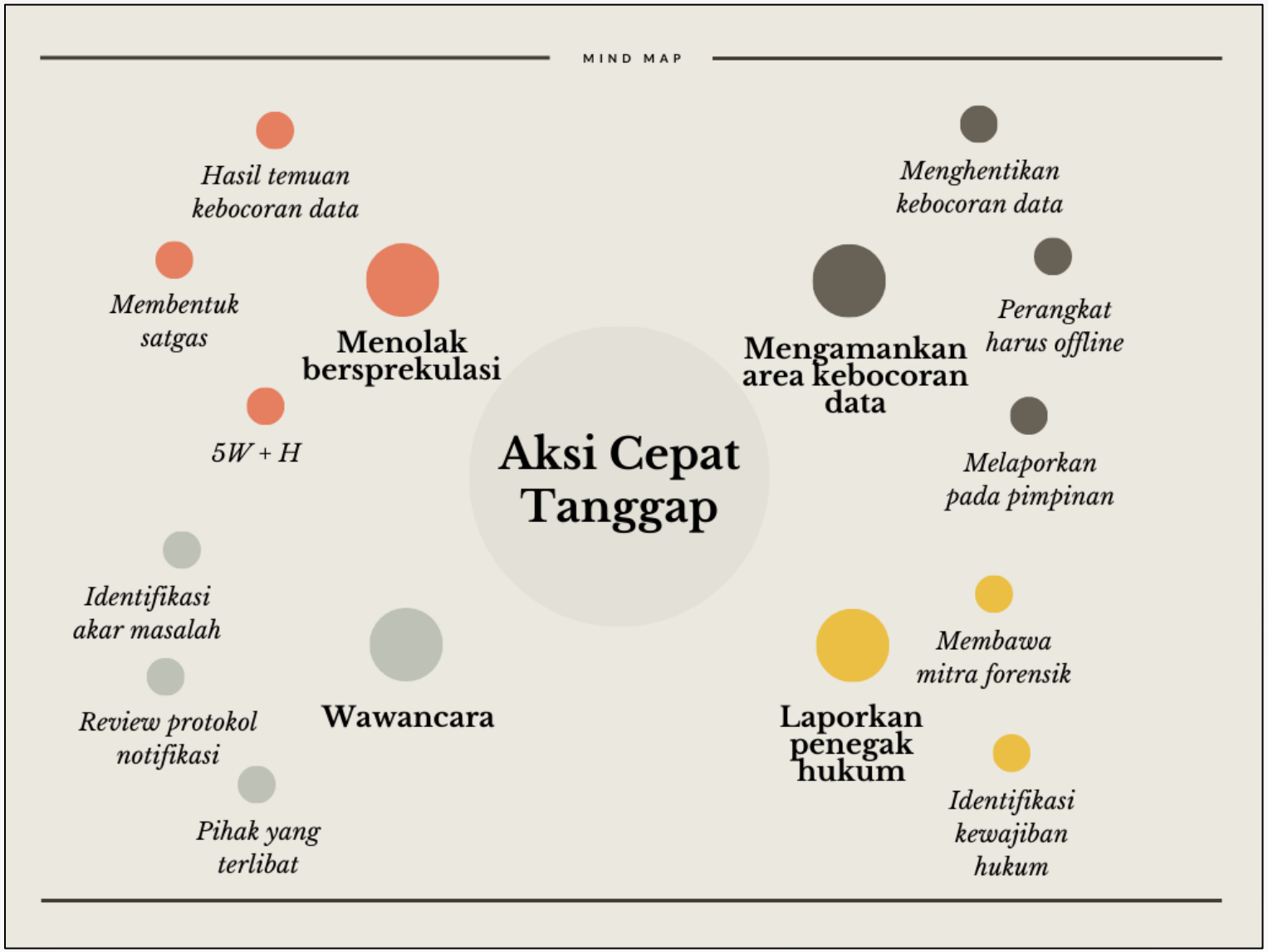
b. Kelalaian

Kebocoran data disebabkan karena tidak memadainya sistem keamanan yang dimiliki. Hal ini termasuk juga tidak diterapkannya sistem atau protokol pengamanan dasar untuk pencegahan terjadinya kebocoran data.

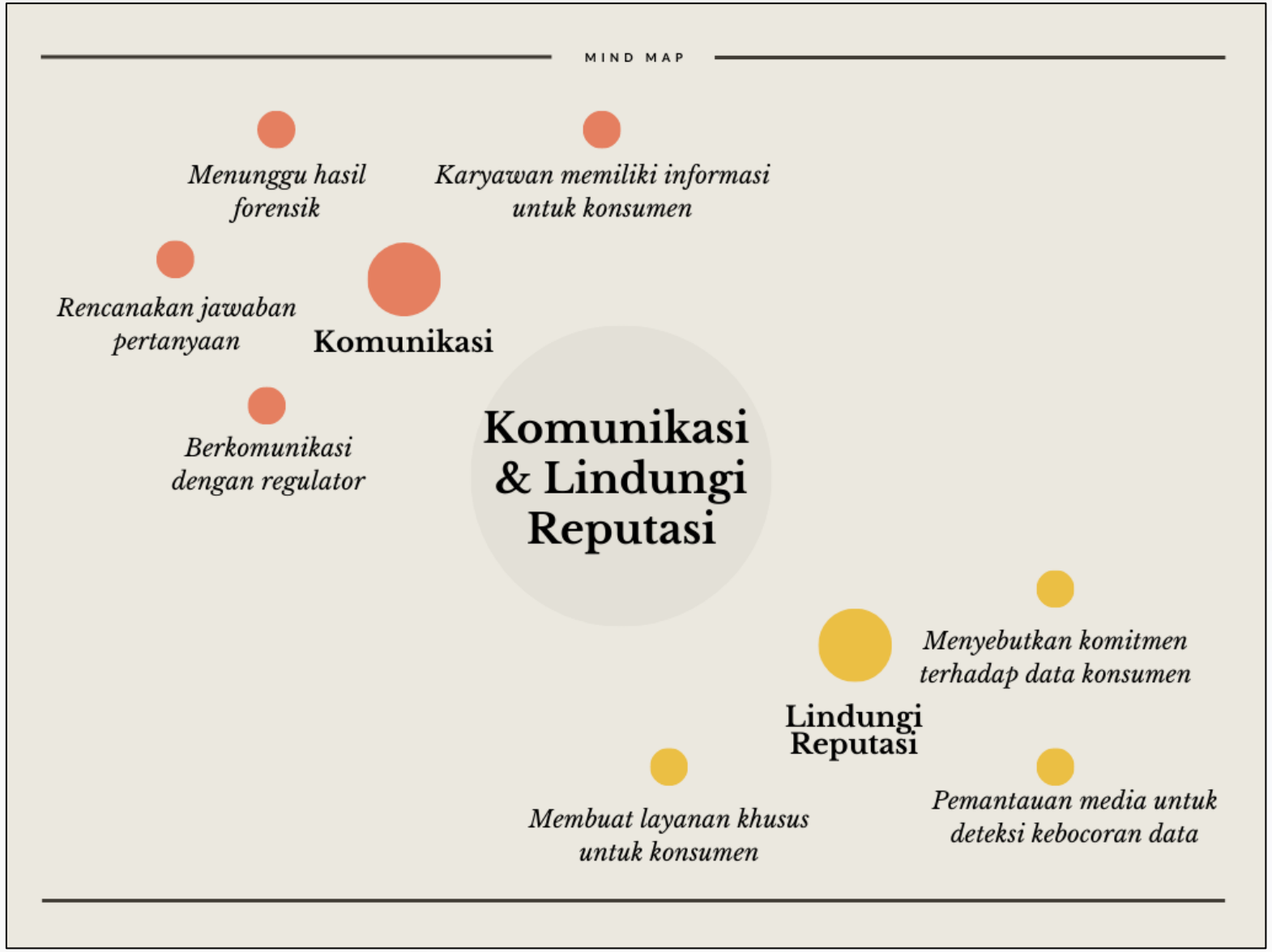
CARA PENANGANAN (PROSES TANGGAP INSIDEN)

a. Aksi Cepat Tanggap
b. Komunikasi dan Lindungi Reputasi
c. Layanan Konsumen

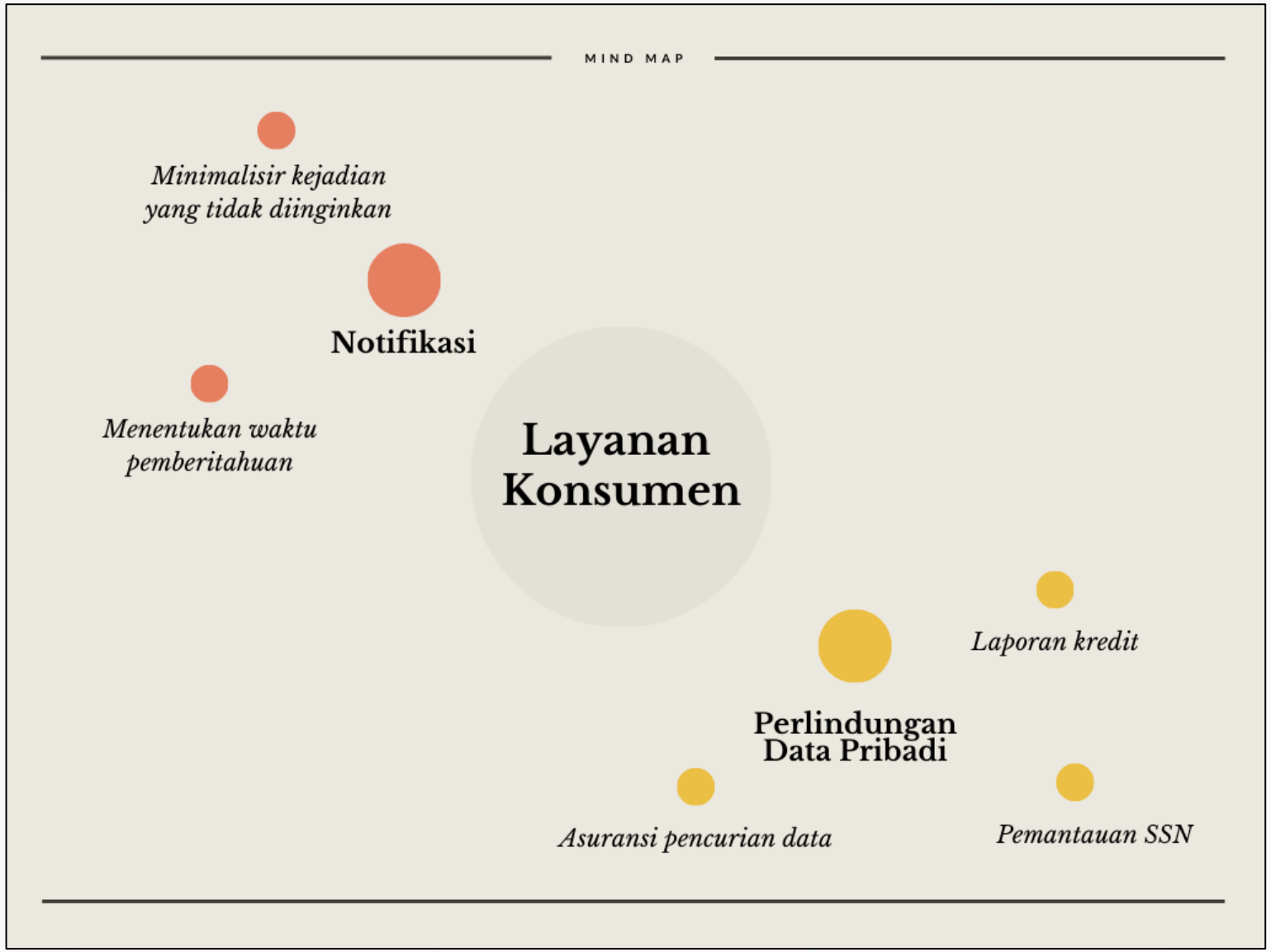
AKSI CEPAT TANGGAP



KOMUNIKASI & LINDUNGI REPUTASI



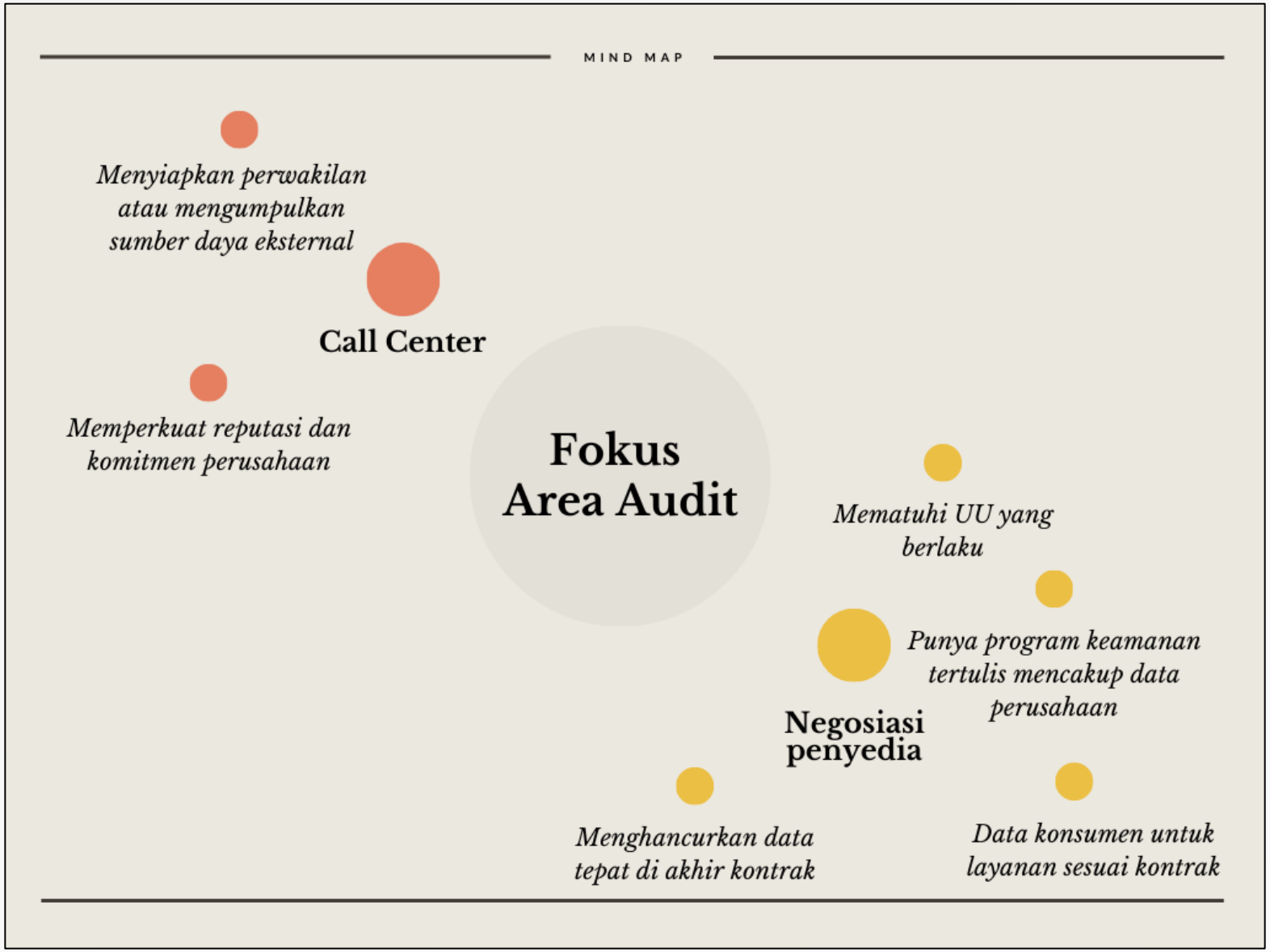
LAYANAN KONSUMEN



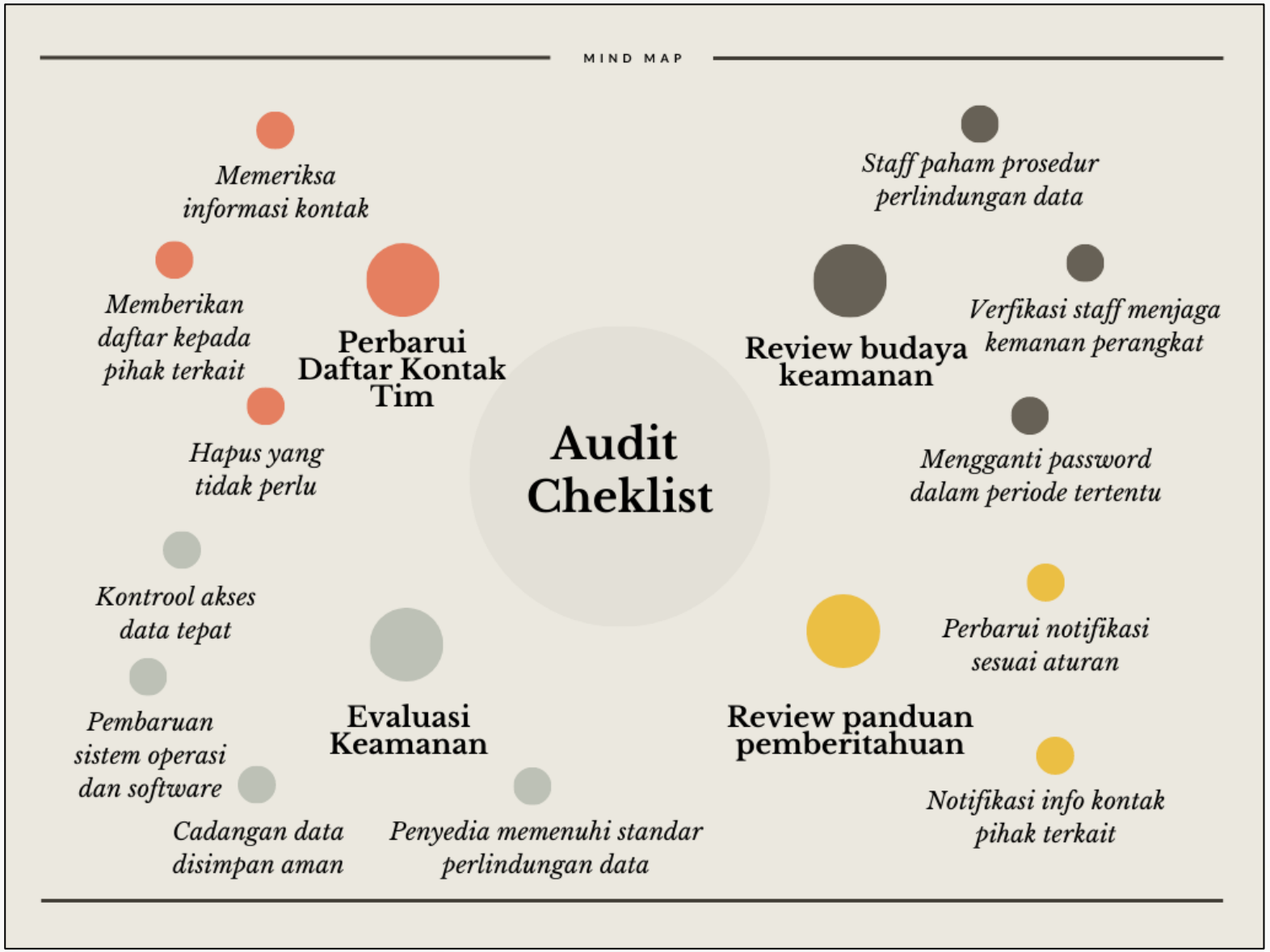
PELAKSANAAN AUDIT DATA

a. Setelah membuat perencanaan, perusahaan harus melakukan audit dan menguji perencanaan yang telah dibuat.
b. Tujuannya adalah untuk membantu mengatasi permasalahan masing-masing, termasuk pelanggaran internal, serangan eksternal, berbagi data tanpa sengaja dan kehilangan/pencurian perangkat fisik.
c. Selalu memperbarui rencana perusahaan untuk menghindari ancaman baru yang tidak terduga yang muncul di waktu yang akan datang.

FOKUS AREA AUDIT



AUDIT CHECKLIST



REKOMENDASI

a. Memberikan tim Pusat Operasi Keamanan (SOC) dengan akses ke intelijen ancaman terbaru dan mendapat informasi terkini tentang alat, teknik serta taktik baru dan terkini yang digunakan oleh aktor ancaman dan pelaku cyber crime.
b. Mengimplementasikan solusi EDR untuk mendeteksi level endpoint, investigasi dan remediasi insiden secara tepat waktu.
c. Menerapkan solusi keamanan tingkat perusahaan yang mendeteksi ancaman lanjutan di tingkat jaringan pada tahap awal.
d. Menerapkan pelatihan dan kegiatan yang mengedukasi karyawan tentang dasar-dasar keamanan cyber.
e. Secara berkala mengingatkan staf bagaimana menangani data sensitif, misal hanya menyimpan layanan cloud terpercaya dengan otentikasi diaktifkan, tidak membaginya kepada pihak ketiga yang tidak dipercaya.
f. Memiliki cadangan data penting dan melakukan pembaruan peralatan dan aplikasi TI secara teratur.
g. Menggunakan produk endpoint khusus yang menuntut manajemen minimum yang memungkinkan karyawan untuk melakukan pekerjaan utama namun tetap terlindung dari malware, ransomware, pengambilalihan akun, penipuan online, dan penipuan.

REFERENSI

[1] AllClear ID: "Data Breach Incident Response Workbook" https://dpoacademy.gr/_files/200000035-ba715bc634/ACID_Self_Service_Incident_Response_Workbook.pdf

[2] Experian: "Data Breach Response Guide" https://www.experian.com/assets/data-breach/brochures/response-guide.pdf

[3] https://id.wikipedia.org/wiki/Ilham_Bintang#:~:text=H.%20Ilham%20Bintang%20(lahir%20di, televisi%20di%20stasiun%20televisi%20swasta

[4] https://megapolitan.kompas.com/read/2020/02/05/13355011/kronologi-dan-peran-8-pelaku-pembobolan-rekening-ilham-bintang?page=all

[5] Panduan Menghadapi Data Breach, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas), Badan Siber dan Sandi Negara (BSSN)

THANK YOU

for your attention

ANALISIS KASUS *DATA BREACH* ILHAM BINTANG

Dosen Pengasuh :

Dr. Widya Cholil, S.Kom., M.IT.

Disusun Oleh :

1. M. Iqbal Rivana (192420057)
2. Isti Ma'atun Nasichah (192420051)
3. Fadel M. Madjid (192420050)

PROGRAM STUDI TEKNIK INFORMATIKA – S2

PROGRAM PASCASARJANA

UNIVERSITAS BINA DARMA

PALEMBANG

KRONOLOGI KEJADIAN

Ilham Bintang, lahir di Makassar, 10 Mei 1955, merupakan seorang wartawan dan pengusaha Indonesia yang dikenal sebagai "pelopor jurnalistik infotainment" di Indonesia dan memiliki 15 slot acara usaha hiburan televisi di stasiun televisi swasta. Saat ini, Ilham Bintang adalah Sekretaris Dewan Kehormatan Persatuan Wartawan Indonesia (PWI) Pusat dan Pemimpin Redaksi Tabloid Cek & Ricek (C&R).

Pada awal tahun 2020 kemarin, wartawan senior Ilham Bintang menjadi pemberitaan banyak media. Penyebabnya adalah insiden penyalahgunaan *simcard* miliknya yang digunakan oleh orang lain saat Ilham Bintang sedang berada di Australia. Pencurian identitas pribadi tersebut berujung pada pembobolan rekening milik Ilham Bintang di Bank Commonwealth yang mengakibatkan hilangnya uang ratusan juta rupiah. Kronologi kasus pembobolan rekening bank Ilham Bintang adalah sebagai berikut:

1. Bermula dari kehilangan sinyal

Dalam sidang, Ilham bintang menceritakan bagaimana ia menyadari bahwa rekeningnya telah dibobol. Semua bermula saat ia sedang berada di Sydney Airport, Australia pada tanggal 4 Januari 2020, di ponsel muncul jaringan SOS, padahal, ia sudah mengaktifkan paket roaming Indosat sebelum berangkat ke Australia. Selang beberapa hari kemudian, tepatnya 6 Januari 2020, jaringan di ponsel Ilham masih menunjukan sinyal SOS. Ilham yang butuh melakukan transaksi perbankan kemudian mengkoneksikan sinyal ponselnya dengan jaringan wifi. Namun, saat itu ia tidak bisa mengakses aplikasi M-Banking dari Bank Commonwelth yang biasa ia gunakan. Ilham memutuskan mendatangi bank Commonwealth yang ada di Melbourne untuk mengkonfirmasi apa yang sedang terjadi. Ternyata uang sebesar 25.000 dollar Australia atau setara 250 juta rupiah telah raib. Kemudian, ia menghubungi agensinya yang berada di Jakarta. Ia meminta agensinya tersebut mengecek uangnya di bank yang sama, namun berbentuk rupiah. Hasilnya pun serupa. Uang sebesar 16 juta rupiah juga telah hilang. Selain itu, terdapat transaksi sebesar 120 juta rupiah di tiga kartu kredit Ilham, yaitu BNI, BCA dan Citibank.

2. Melapor ke Kepolisian Melbourne - Australia

Langkah pertama yang dilakukan Ilham saat itu adalah melapor ke Kepolisian Melbourne karena mengira itu adalah kejahatan internasional karena saat itu uang dalam bentuk dollar Australia. Kemudian Ilham pulang ke Indonesia dan ternyat, sinyal *simcard*-nya masih menghilang. Ia kemudian mendatangi gerai Indosat dan mengetahui bahwa seseorang telah mengambil alih *simcard*-nya. Seseorang yang mengaku sebagai Ilham Bintang mengurus kehilangan nomor ponsel di gerai Indosat di kawasan Bintaro. Setelah mendapatkan *simcard* itu, barulah mereka bisa mengakses berbagai rekening bank tersebut. Ilham kemudian melaporkan hal tersebut ke kepolisian setempat hingga akhirnya komplotan pelaku ditangkap.

Peran para tersangka :

a. Tersangka D, di tangkap di palembang. D berperan sebagai bos dari sindikat ini. Dia membeli data-data nasabah bank dan slip OJK untuk mengetahui data-data korban sebagai targetnya. D bertugas memastikan ponsel Ilham Bintang tetap dalam kondisi mati agar para pelaku bisa membuat SIM card dengan data korban.

b. Tersangka H, pegawai Bank, H yang menjual data-data korban. Tersangka H punya akses bisa mendapat slip OJK. Di situ ada data-data pribadi lengkap seseorang yang memiliki rekening atau limit rekening.

c. Tersangka R dan HN yang berperan membantu H untuk menyiapkan data-data yang dijual.

d. Tersangka W, AY dan TR yang berada di Jakarta untuk menduplikat *simcard* korban dengan cara datang langsung ke gerai Indosat di Jakarta Barat.

e. Tersangka JW yang membuat KTP palsu dari Ilham Bintang dengan foto yang tertera foto orang lain

Dari *simcard* tersebut, D mulai menelisik email hingga akun m-banking milik Ilham. D mulai masuk ke aplikasi *Yahoo* untuk mengetahui email Ilham. Saat diminta me-*reset* (untuk membuka email Ilham), dikirim OTP (*One Time Password*) ke nomor telepon baru. Jadi *password* email pribadi Ilham dapat diganti. Setelah email terbuka, terbuka juga data bank, sehingga dua rekening habis terkuras.

3. Menyalahkan pihak Indosat

Dalam persidangan tersebut, Ilham sempat menyalahkan operator penyedia layanan kartu perdana Indosat karena dianggap melakukan kelalaian hingga rekeningnya berhasil dibobol. Menurut Ilham, pegawai Indosat di gerai Bintaro telah melakukan kelalaian sehingga nomor ponselnya bisa diambil alih oleh para terdakwa. Selain heran dengan waktu pengurusan penggantian *simcard* yang cepat, Ilham juga mendapat keterangan dari Indosat bahwa mereka lupa membuat salinan KTP yang digunakan para tersangka. Ia menyalahkan pihak Indosat karena dianggap tidak menjalankan penggantian nomor ponsel sesuai SOP yang seharusnya.

4. Terdakwa membantah membobol kartu kredit

Salah satu terdakwa dalam kasus tersebut membantah bahwa ia yang membobol kartu kredit BCA korban. Ia mengakui bahwa ia mengambil uang ratusan juta dari rekening Bank Commonwealth. Namun, hakim tidak terlalu mempermasalahkan hal tersebut karena pada akhirnya pihak bank berhasil membatalkan seluruh transaksi melalui kartu kredit Ilham. Kerugian yang dirasakan Ilham hanya berasal dari pembobolan di bank Commonwealth yang membuatnya kehilangan uang senilai 265 juta rupiah.

5. Hakim memberikan teguran kepada jaksa

Dalam persidangan kemarin sempat diwarnai beberapa teguran hakim kepada jaksa. Jaksa Penuntut Umum (JPU) Mudjiono ditegur karena tidak membawa barang bukti yang diperlukan serta tidak masuknya sejumlah saksi dalam persidangan tersebut. Teguran pertama dilayangkan Kamaludin ketika ia meminta barang bukti berupa surat keterangan dari pihak Indosat. Namun setelah mengecek serangkaian barang bukti yang ia pegang, Mudjiono mengaku tidak membawanya. Hakim kemudian menanyakan apakah foto copy KTP Ilham Bintang yang menjadi barang bukti di sidang terdakwa lainnya juga menjadi barang bukti dalam kasus tersebut. Namun, JPU menyebutkan bahwa foto copy KTP tersebut tidak dicantumkan. Karena kesalahan jaksa tersebut, majelis hakim terpaksa meminta Ilham Bintang untuk kembali hadir dalam persidangan selanjutnya.

Kemudian, hakim juga sempat menanyakan kepada Jaksa apakah terdakwa pembuat KTP palsu yang disidangkan terpisah menjadi saksi dalam sidang tersebut.

Setelah mengecek daftar saksi, Mudjianto menyampaikan bahwa ia tidak memasukkannya kedalam daftar saksi. Adapun dalam persidangan tersebut, terdapat lima orang terdakwa yang menjalani persidangan. Lima terdakwa itu antara lain Desar (20), Teti Rosmiawati (46), Wasno (52), Amran Yunianto (53), dan Pegik (28). Sementara tiga terdakwa lainnya yang terlibat dalam komplotan tersebut disidang secara terpisah di Pengadilan Negeri Jakarta Barat. Mereka didakwa dengan Pasal 35 juncto Pasal 51 ayat 1 juncto Pasal 30 juncto Pasal 46 ayat 1 UU RI 11 Tahun 2008 tentang ITE dan atau Pasal 363 KUHP, Pasal 263 KUHP, Pasal 3 dan 4 juncto Pasal 10 UU RI nomor 8 tahun 2010 tentang pencegahan dan pemberantasan tindak pidana pencucian uang.

KERUGIAN

Dari kejadian pembobolan rekening bank Ilham Bintang tersebut dapat mengakibatkan kerugian-kerugian yang bersifat materil maupun immateril bagi korban, antara lain sebagai berikut :

1. Kerugian materil hingga nominal 265 juta rupiah.
2. Ketidaknyamanan atas tindakan cybercrime (pencurian data pribadi) pada pihak korban sebagai pengguna.
3. Trauma atau efek psikologis pada korban.
4. Hilangnya kepercayaan terhadap sistem keamanan dan hukum di Indonesia.

Kerugian tidak hanya dialami oleh Ilham Bintang saja, namun juga dirasakan oleh pihak Indosat dan Bank Commonwealth, yaitu :

1. Hilangnya reputasi, kredibilitas, integritas dan kepercayaan dari masyarakat yang berdampak dalam waktu yang cukup lama.
2. Berdampak buruk pada lini keuangan dalam organisasi
3. Terlibat dalam kasus hukum yang rumit dan panjang serta berisiko terkena denda karena pelanggaran hukum perdata.

CARA PENANGANAN

1. Identifikasi

Berdasarkan kasus Ilham Bintang, dapat diidentifikasi 2 jenis cara bagaimana kebocoran data dapat terjadi, yaitu :

a. Keterlibatan Orang Dalam

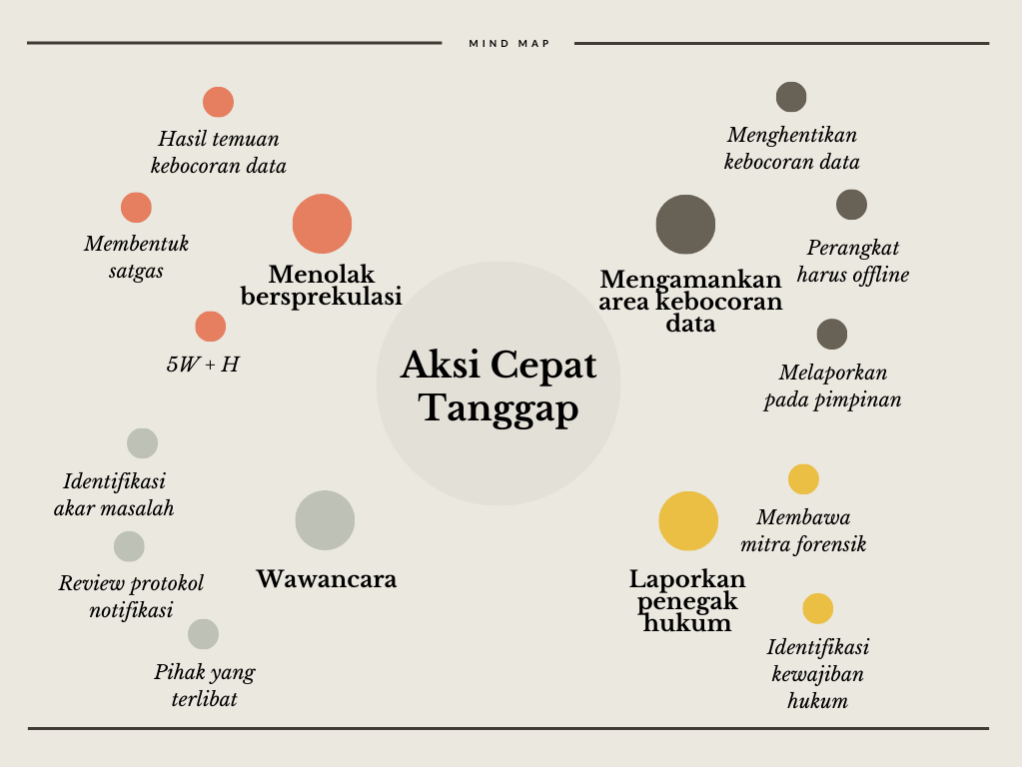
Kebocoran data disebabkan oleh karyawan sebuah institusi itu sendiri, mantan karyawan, atau oleh karyawan yang berhasil dikelabui dengan *social engineering* sehingga tanpa sadar ia memberikan data ataupun akses terhadap data.

b. Kelalaian

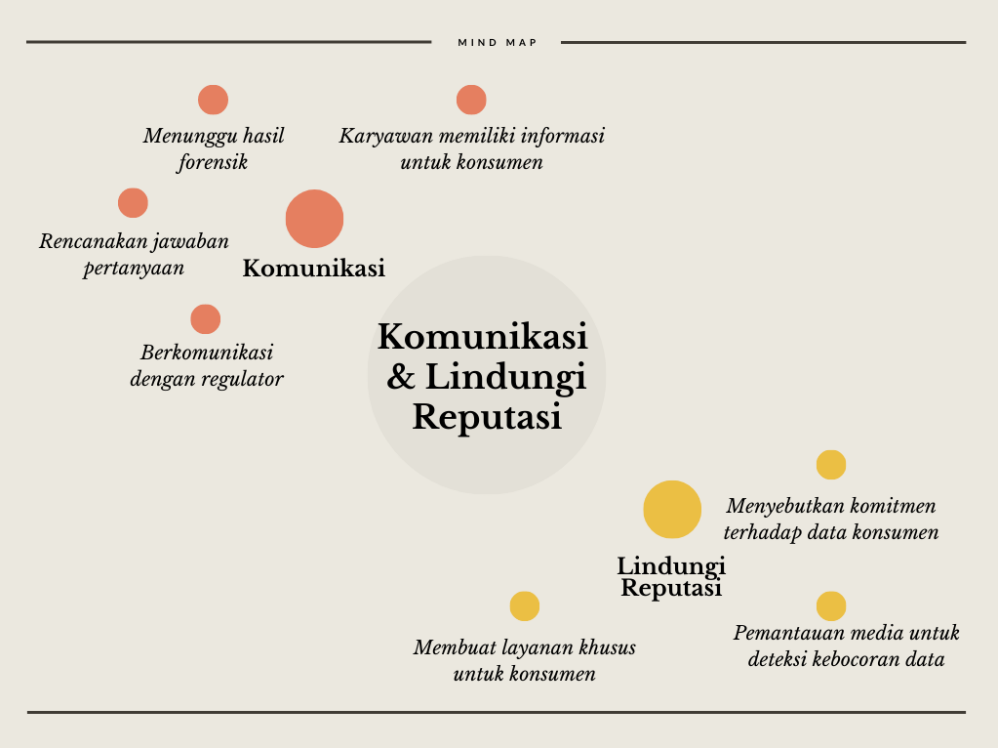
Kebocoran data disebabkan karena tidak memadainya sistem keamanan yang dimiliki. Hal ini termasuk juga tidak diterapkannya sistem atau protokol pengamanan dasar untuk pencegahan terjadinya kebocoran data.

2. Cara Penanganan (Proses Tanggap Insiden)

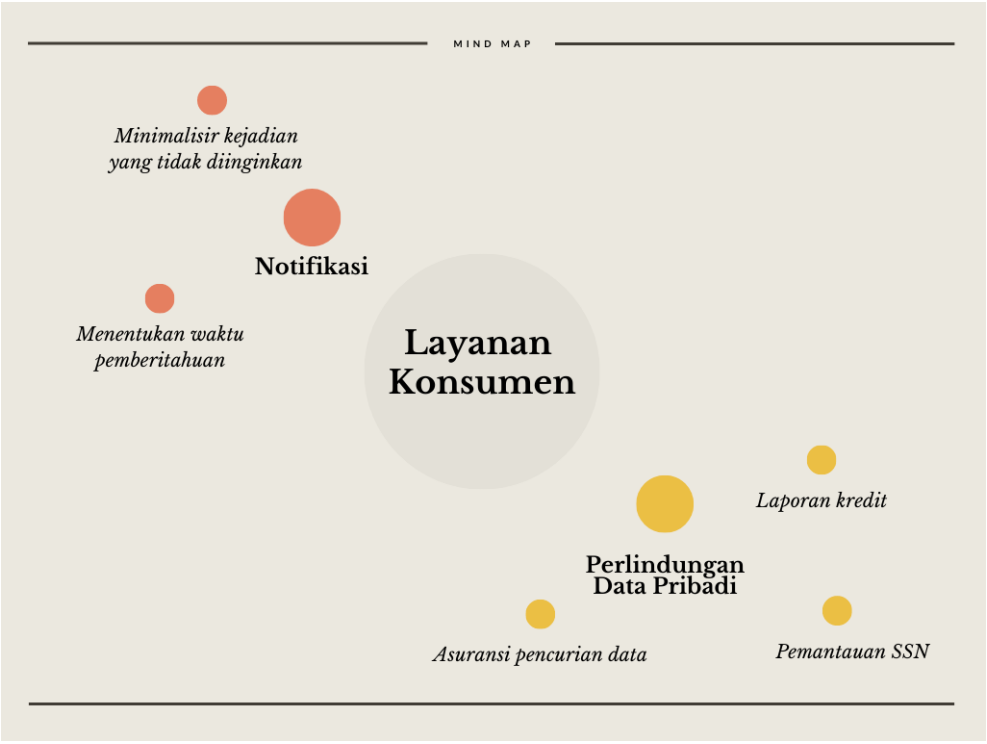
a. Aksi Cepat Tanggap



b. Komunikasi dan Lindungi Reputasi



c. Layanan Konsumen

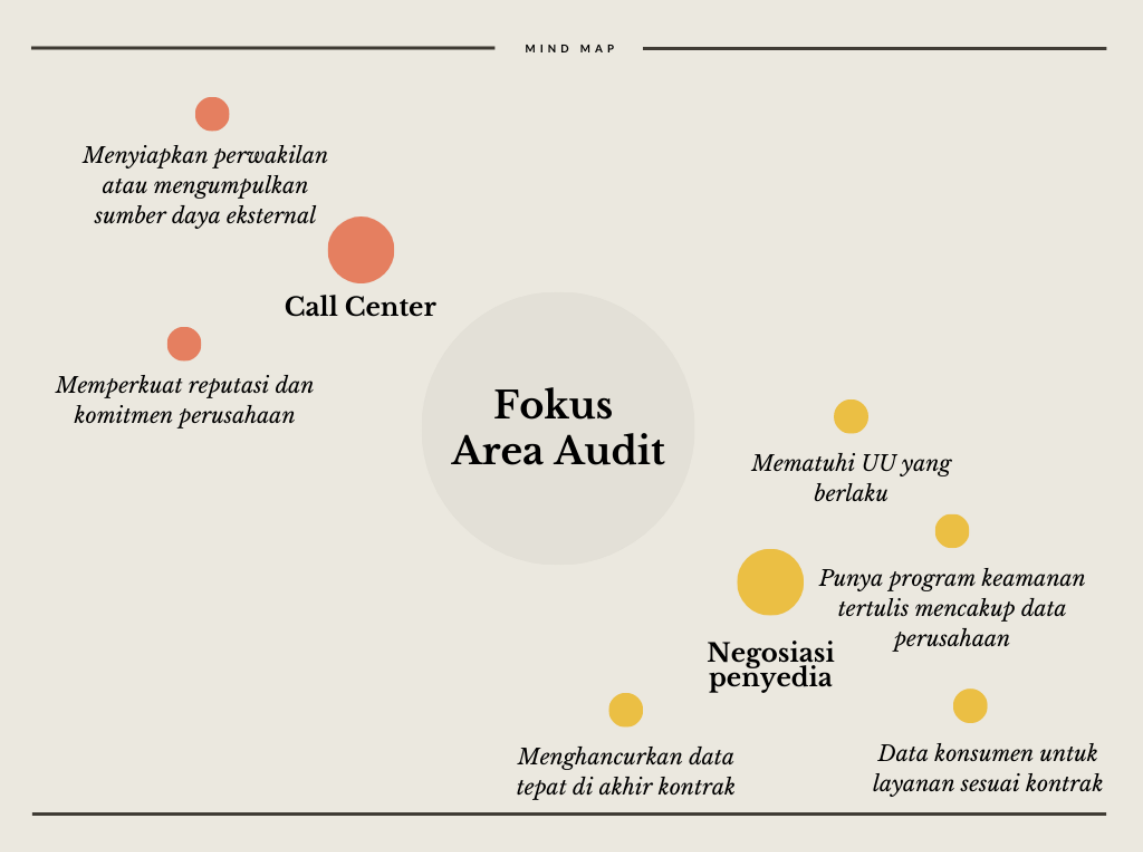


PELAKSANAAN AUDIT DATA

Setelah membuat perencanaan, perusahaan harus melakukan audit dan menguji perencanaan yang telah dibuat. Tujuannya adalah untuk membantu mengatasi permasalahan masing-masing, termasuk pelanggaran internal, serangan eksternal, berbagi data tanpa sengaja dan kehilangan/pencurian perangkat fisik. Selain itu, juga perlu untuk selalu memperbarui rencana perusahaan untuk menghindari ancaman baru yang tidak terduga yang muncul di waktu yang akan datang.

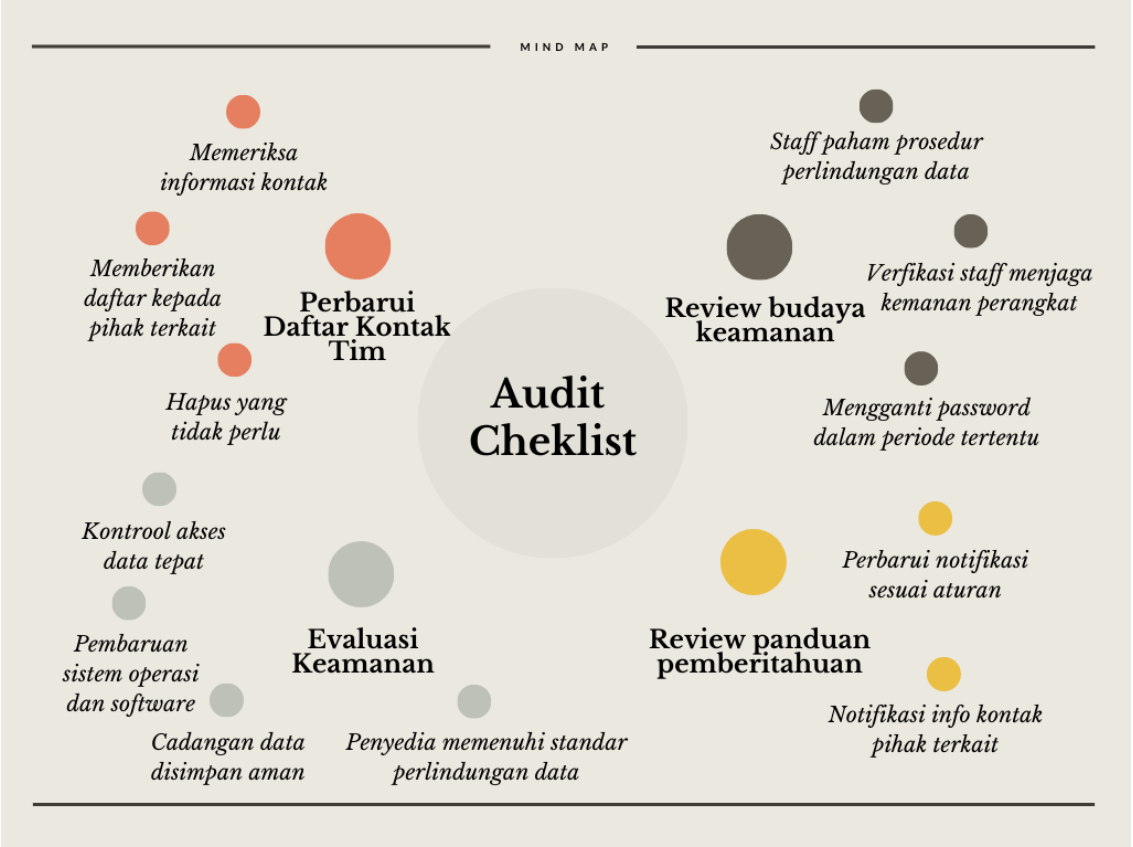
1. Fokus Area

Berikut ini adalah beberapa area yang dilaksanakan audit, yaitu :



2. Audit Checklist

Berikut ini adalah langkah yang dilakukan pada saat audit sesuai ruang lingkup respon perusahaan, yaitu :


MIND MAP
Audit Cheklist
Memeriksa informasi kontak
Memberikan daftar kepada pihak terkait
Perbarui Daftar Kontak Tim
Hapus yang tidak perlu
Kontrool akses data tepat
Pembaruan sistem operasi dan software
Evaluasi Keamanan
Cadangan data disimpan aman
Penyedia memenuhi standar perlindungan data
Staff paham prosedur perlindungan data
Review budaya keamanan
Verfikasi staff menjaga kemanan perangkat
Mengganti password dalam periode tertentu
Perbarui notifikasi sesuai aturan
Review panduan pemberitahuan
Notifikasi info kontak pihak terkait

REKOMENDASI

a. Memberikan tim Pusat Operasi Keamanan (SOC) dengan akses ke intelijen ancaman terbaru dan mendapatkan informasi terkini tentang alat, teknik serta taktik baru dan terkini yang digunakan oleh aktor ancaman dan pelaku *cyber crime*.
b. Mengimplementasikan solusi EDR untuk mendeteksi level *endpoint*, investigasi, dan remediasi insiden secara tepat waktu.
c. Selain mengadopsi perlindungan *endpoint* yang penting, juga perlu menerapkan solusi keamanan tingkat perusahaan yang mendeteksi ancaman lanjutan di tingkat jaringan pada tahap awal.
d. Menerapkan pelatihan dan kegiatan yang mengedukasi karyawan tentang dasar-dasar keamanan *cyber*, misalnya tidak membuka atau menyimpan file dari email atau situs web yang tidak dikenal karena dapat membahayakan seluruh perusahaan.
e. Secara berkala mengingatkan staf bagaimana menangani data sensitif, misalnya hanya menyimpan layanan cloud terpercaya dengan otentikasi diaktifkan, tidak membaginya kepada pihak ketiga yang tidak dipercaya.
f. Memiliki cadangan data penting dan melakukan pembaruan peralatan dan aplikasi TI secara teratur untuk menghindari kerentanan yang tidak tertandingi yang dapat menjadi alasan terjadinya pelanggaran.
g. Menggunakan produk *endpoint* khusus yang menuntut manajemen minimum yang memungkinkan karyawan untuk melakukan pekerjaan utama mereka namun tetap terlindung dari malware, ransomware, pengambilalihan akun, penipuan online, dan penipuan.

REFERENSI

[1] AllClear ID: "Data Breach Incident Response Workbook" https://dpoacademy.gr/_files/20000003-ba715bc634/ACID_Self_Service_Incident_Response_Workbook.pdf

[2] Experian: "Data Breach Response Guide" https://www.experian.com/assets/data-breach/brochures/response-guide.pdf

[3] https://id.wikipedia.org/wiki/Ilham_Bintang#:~:text=H.%20Ilham%20Bintang%20(lahir%20di,televisi%20di%20stasiun%20televisi%20swasta

[4] https://megapolitan.kompas.com/read/2020/02/05/13355011/kronologi-dan-peran-8-pelaku-pembobolan-rekening-ilham-bintang?page=all

[5] Panduan Menghadapi Data Breach, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas), Badan Siber dan Sandi Negara (BSSN)

ANALISIS KASUS *DATA BREACH* ILHAM BINTANG

Dosen Pengasuh :

Dr. Widya Cholil, S.Kom., M.IT.

Disusun Oleh :

1. M. Iqbal Rivana (192420057)
2. Isti Ma'atun Nasichah (192420051)
3. Fadel M. Madjid (192420050)

PROGRAM STUDI TEKNIK INFORMATIKA – S2

PROGRAM PASCASARJANA

UNIVERSITAS BINA DARMA

PALEMBANG

KRONOLOGI KEJADIAN

Ilham Bintang, lahir di Makassar, 10 Mei 1955, merupakan seorang wartawan dan pengusaha Indonesia yang dikenal sebagai "pelopor jurnalistik infotainment" di Indonesia dan memiliki 15 slot acara usaha hiburan televisi di stasiun televisi swasta. Saat ini, Ilham Bintang adalah Sekretaris Dewan Kehormatan Persatuan Wartawan Indonesia (PWI) Pusat dan Pemimpin Redaksi Tabloid Cek & Ricek (C&R).

Pada awal tahun 2020 kemarin, wartawan senior Ilham Bintang menjadi pemberitaan banyak media. Penyebabnya adalah insiden penyalahgunaan *simcard* miliknya yang digunakan oleh orang lain saat Ilham Bintang sedang berada di Australia. Pencurian identitas pribadi tersebut berujung pada pembobolan rekening milik Ilham Bintang di Bank Commonwealth yang mengakibatkan hilangnya uang ratusan juta rupiah. Kronologi kasus pembobolan rekening bank Ilham Bintang adalah sebagai berikut:

1. Bermula dari kehilangan sinyal

Dalam sidang, Ilham bintang menceritakan bagaimana ia menyadari bahwa rekeningnya telah dibobol. Semua bermula saat ia sedang berada di Sydney Airport, Australia pada tanggal 4 Januari 2020, di ponsel muncul jaringan SOS, padahal, ia sudah mengaktifkan paket roaming Indosat sebelum berangkat ke Australia. Selang beberapa hari kemudian, tepatnya 6 Januari 2020, jaringan di ponsel Ilham masih menunjukan sinyal SOS. Ilham yang butuh melakukan transaksi perbankan kemudian mengkoneksikan sinyal ponselnya dengan jaringan wifi. Namun, saat itu ia tidak bisa mengakses aplikasi M-Banking dari Bank Commonwelth yang biasa ia gunakan. Ilham memutuskan mendatangi bank Commonwealth yang ada di Melbourne untuk mengkonfirmasi apa yang sedang terjadi. Ternyata uang sebesar 25.000 dollar Australia atau setara 250 juta rupiah telah raib. Kemudian, ia menghubungi agensinya yang berada di Jakarta. Ia meminta agensinya tersebut mengecek uangnya di bank yang sama, namun berbentuk rupiah. Hasilnya pun serupa. Uang sebesar 16 juta rupiah juga telah hilang. Selain itu, terdapat transaksi sebesar 120 juta rupiah di tiga kartu kredit Ilham, yaitu BNI, BCA dan Citibank.

2. Melapor ke Kepolisian Melbourne - Australia

Langkah pertama yang dilakukan Ilham saat itu adalah melapor ke Kepolisian Melbourne karena mengira itu adalah kejahatan internasional karena saat itu uang dalam bentuk dollar Australia. Kemudian Ilham pulang ke Indonesia dan ternyat, sinyal *simcard*-nya masih menghilang. Ia kemudian mendatangi gerai Indosat dan mengetahui bahwa seseorang telah mengambil alih *simcard*-nya. Seseorang yang mengaku sebagai Ilham Bintang mengurus kehilangan nomor ponsel di gerai Indosat di kawasan Bintaro. Setelah mendapatkan *simcard* itu, barulah mereka bisa mengakses berbagai rekening bank tersebut. Ilham kemudian melaporkan hal tersebut ke kepolisian setempat hingga akhirnya komplotan pelaku ditangkap.

Peran para tersangka :

a. Tersangka D, di tangkap di palembang. D berperan sebagai bos dari sindikat ini. Dia membeli data-data nasabah bank dan slip OJK untuk mengetahui data-data korban sebagai targetnya. D bertugas memastikan ponsel Ilham Bintang tetap dalam kondisi mati agar para pelaku bisa membuat SIM card dengan data korban.

b. Tersangka H, pegawai Bank, H yang menjual data-data korban. Tersangka H punya akses bisa mendapat slip OJK. Di situ ada data-data pribadi lengkap seseorang yang memiliki rekening atau limit rekening.

c. Tersangka R dan HN yang berperan membantu H untuk menyiapkan data-data yang dijual.

d. Tersangka W, AY dan TR yang berada di Jakarta untuk menduplikat *simcard* korban dengan cara datang langsung ke gerai Indosat di Jakarta Barat.

e. Tersangka JW yang membuat KTP palsu dari Ilham Bintang dengan foto yang tertera foto orang lain

Dari *simcard* tersebut, D mulai menelisik email hingga akun m-banking milik Ilham. D mulai masuk ke aplikasi *Yahoo* untuk mengetahui email Ilham. Saat diminta me-*reset* (untuk membuka email Ilham), dikirim OTP (*One Time Password*) ke nomor telepon baru. Jadi *password* email pribadi Ilham dapat diganti. Setelah email terbuka, terbuka juga data bank, sehingga dua rekening habis terkuras.

3. Menyalahkan pihak Indosat

Dalam persidangan tersebut, Ilham sempat menyalahkan operator penyedia layanan kartu perdana Indosat karena dianggap melakukan kelalaian hingga rekeningnya berhasil dibobol. Menurut Ilham, pegawai Indosat di gerai Bintaro telah melakukan kelalaian sehingga nomor ponselnya bisa diambil alih oleh para terdakwa. Selain heran dengan waktu pengurusan penggantian *simcard* yang cepat, Ilham juga mendapat keterangan dari Indosat bahwa mereka lupa membuat salinan KTP yang digunakan para tersangka. Ia menyalahkan pihak Indosat karena dianggap tidak menjalankan penggantian nomor ponsel sesuai SOP yang seharusnya.

4. Terdakwa membantah membobol kartu kredit

Salah satu terdakwa dalam kasus tersebut membantah bahwa ia yang membobol kartu kredit BCA korban. Ia mengakui bahwa ia mengambil uang ratusan juta dari rekening Bank Commonwealth. Namun, hakim tidak terlalu mempermasalahkan hal tersebut karena pada akhirnya pihak bank berhasil membatalkan seluruh transaksi melalui kartu kredit Ilham. Kerugian yang dirasakan Ilham hanya berasal dari pembobolan di bank Commonwealth yang membuatnya kehilangan uang senilai 265 juta rupiah.

5. Hakim memberikan teguran kepada jaksa

Dalam persidangan kemarin sempat diwarnai beberapa teguran hakim kepada jaksa. Jaksa Penuntut Umum (JPU) Mudjiono ditegur karena tidak membawa barang bukti yang diperlukan serta tidak masuknya sejumlah saksi dalam persidangan tersebut. Teguran pertama dilayangkan Kamaludin ketika ia meminta barang bukti berupa surat keterangan dari pihak Indosat. Namun setelah mengecek serangkaian barang bukti yang ia pegang, Mudjiono mengaku tidak membawanya. Hakim kemudian menanyakan apakah foto copy KTP Ilham Bintang yang menjadi barang bukti di sidang terdakwa lainnya juga menjadi barang bukti dalam kasus tersebut. Namun, JPU menyebutkan bahwa foto copy KTP tersebut tidak dicantumkan. Karena kesalahan jaksa tersebut, majelis hakim terpaksa meminta Ilham Bintang untuk kembali hadir dalam persidangan selanjutnya.

Kemudian, hakim juga sempat menanyakan kepada Jaksa apakah terdakwa pembuat KTP palsu yang disidangkan terpisah menjadi saksi dalam sidang tersebut.

Setelah mengecek daftar saksi, Mudjianto menyampaikan bahwa ia tidak memasukkannya kedalam daftar saksi. Adapun dalam persidangan tersebut, terdapat lima orang terdakwa yang menjalani persidangan. Lima terdakwa itu antara lain Desar (20), Teti Rosmiawati (46), Wasno (52), Amran Yunianto (53), dan Pegik (28). Sementara tiga terdakwa lainnya yang terlibat dalam komplotan tersebut disidang secara terpisah di Pengadilan Negeri Jakarta Barat. Mereka didakwa dengan Pasal 35 juncto Pasal 51 ayat 1 juncto Pasal 30 juncto Pasal 46 ayat 1 UU RI 11 Tahun 2008 tentang ITE dan atau Pasal 363 KUHP, Pasal 263 KUHP, Pasal 3 dan 4 juncto Pasal 10 UU RI nomor 8 tahun 2010 tentang pencegahan dan pemberantasan tindak pidana pencucian uang.

KERUGIAN

Dari kejadian pembobolan rekening bank Ilham Bintang tersebut dapat mengakibatkan kerugian-kerugian yang bersifat materil maupun immateril bagi korban, antara lain sebagai berikut :

1. Kerugian materil hingga nominal 265 juta rupiah.
2. Ketidaknyamanan atas tindakan cybercrime (pencurian data pribadi) pada pihak korban sebagai pengguna.
3. Trauma atau efek psikologis pada korban.
4. Hilangnya kepercayaan terhadap sistem keamanan dan hukum di Indonesia.

Kerugian tidak hanya dialami oleh Ilham Bintang saja, namun juga dirasakan oleh pihak Indosat dan Bank Commonwealth, yaitu :

1. Hilangnya reputasi, kredibilitas, integritas dan kepercayaan dari masyarakat yang berdampak dalam waktu yang cukup lama.
2. Berdampak buruk pada lini keuangan dalam organisasi
3. Terlibat dalam kasus hukum yang rumit dan panjang serta berisiko terkena denda karena pelanggaran hukum perdata.

CARA PENANGANAN

1. Identifikasi

Berdasarkan kasus Ilham Bintang, dapat diidentifikasi 2 jenis cara bagaimana kebocoran data dapat terjadi, yaitu :

a. Keterlibatan Orang Dalam

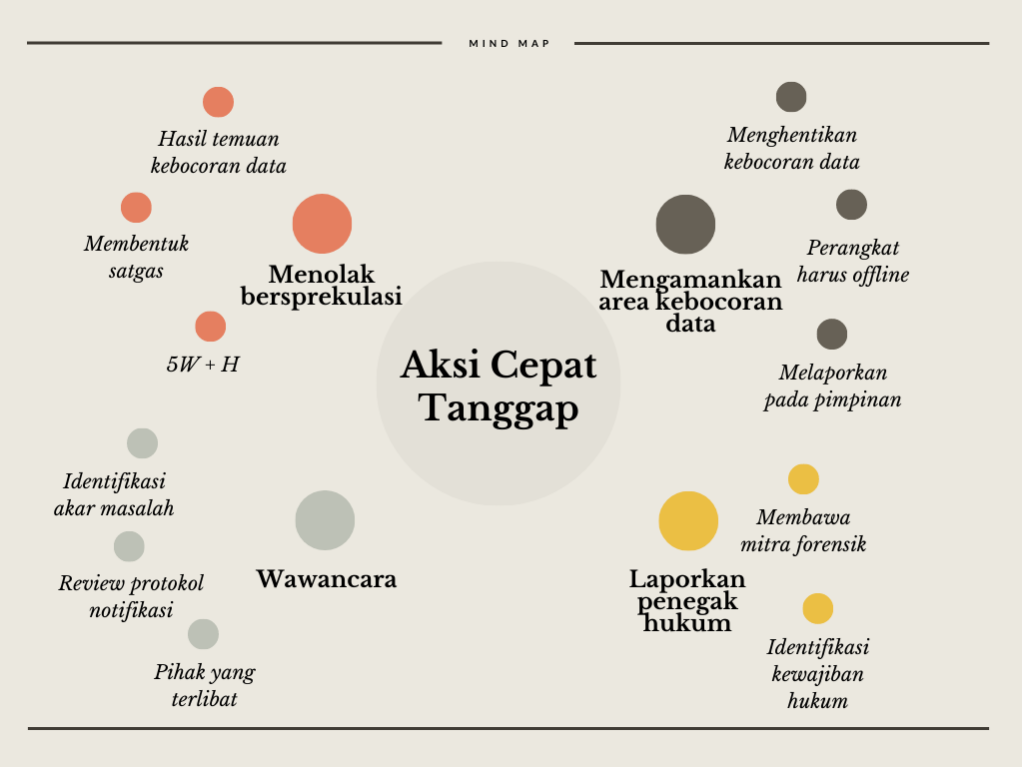
Kebocoran data disebabkan oleh karyawan sebuah institusi itu sendiri, mantan karyawan, atau oleh karyawan yang berhasil dikelabui dengan *social engineering* sehingga tanpa sadar ia memberikan data ataupun akses terhadap data.

b. Kelalaian

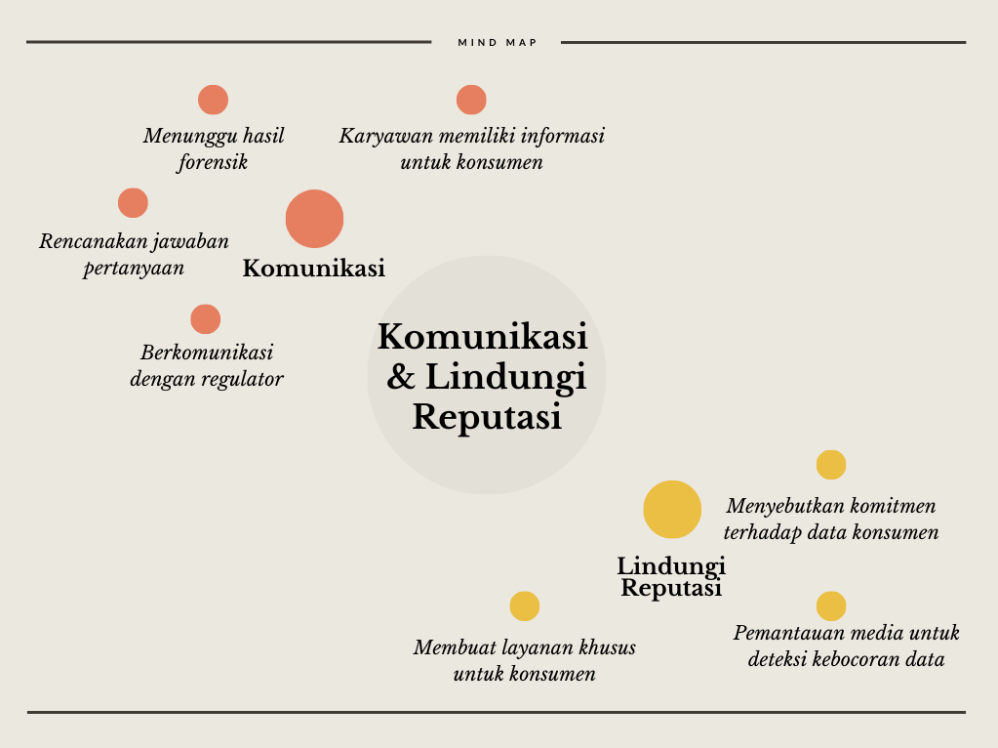
Kebocoran data disebabkan karena tidak memadainya sistem keamanan yang dimiliki. Hal ini termasuk juga tidak diterapkannya sistem atau protokol pengamanan dasar untuk pencegahan terjadinya kebocoran data.

2. Cara Penanganan (Proses Tanggap Insiden)

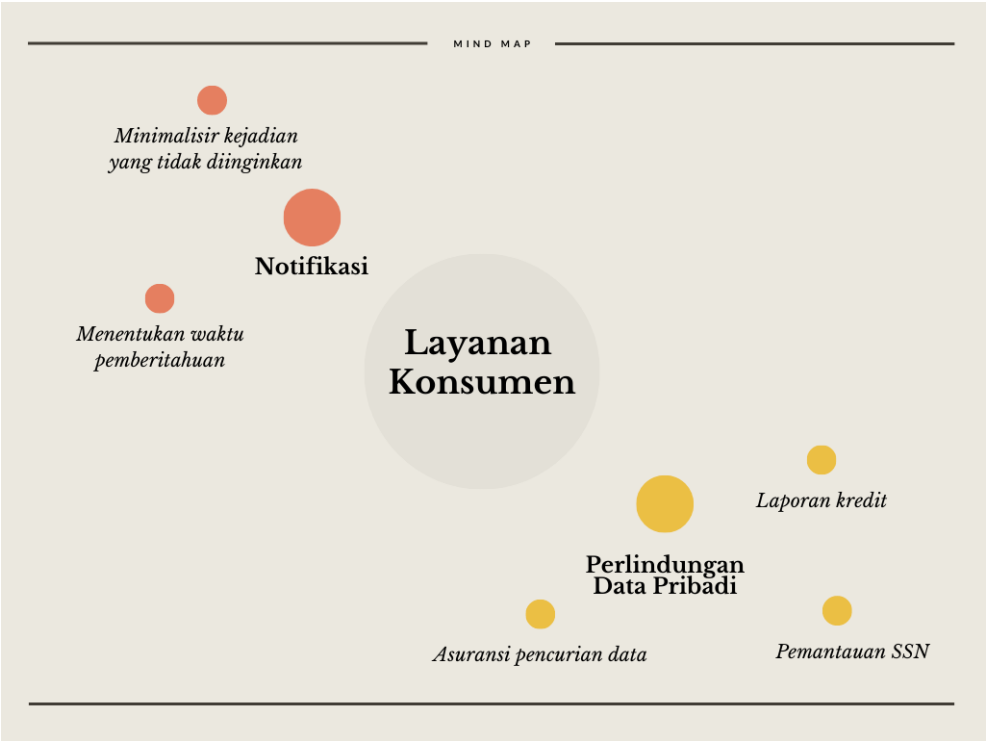
a. Aksi Cepat Tanggap



b. Komunikasi dan Lindungi Reputasi



c. Layanan Konsumen

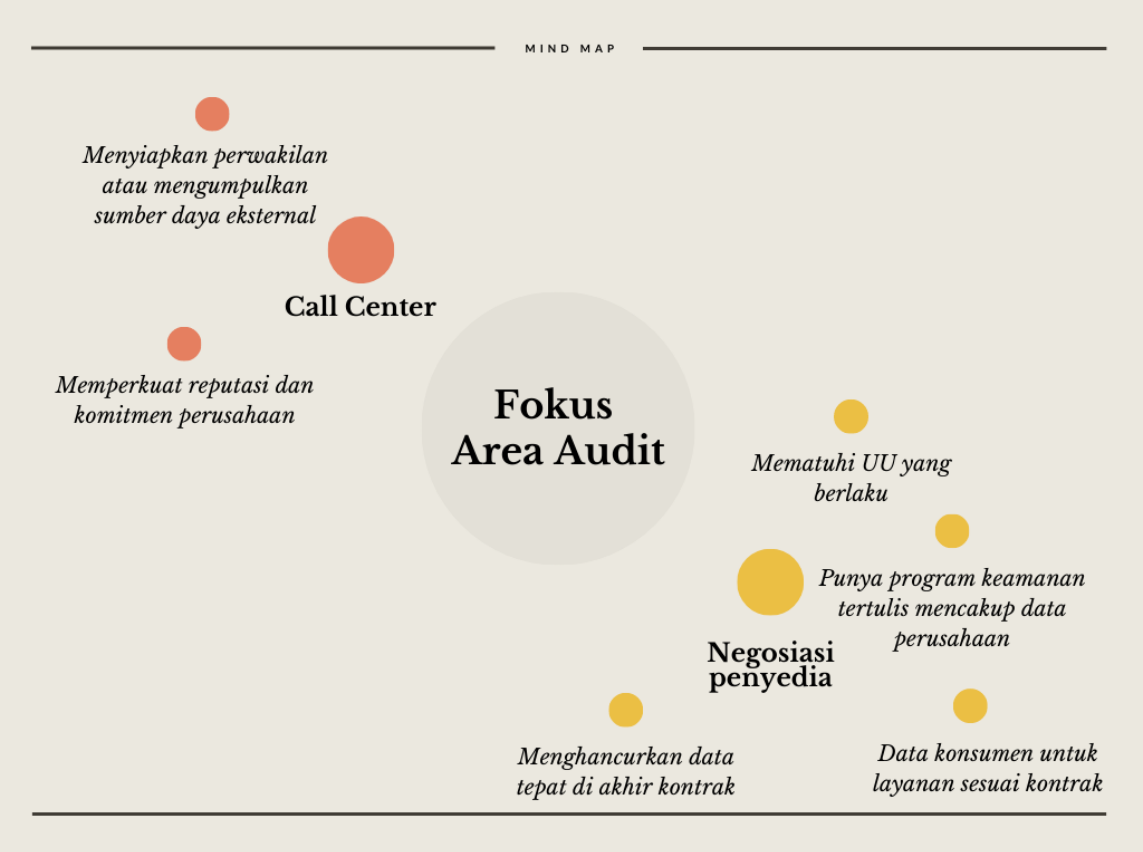


PELAKSANAAN AUDIT DATA

Setelah membuat perencanaan, perusahaan harus melakukan audit dan menguji perencanaan yang telah dibuat. Tujuannya adalah untuk membantu mengatasi permasalahan masing-masing, termasuk pelanggaran internal, serangan eksternal, berbagi data tanpa sengaja dan kehilangan/pencurian perangkat fisik. Selain itu, juga perlu untuk selalu memperbarui rencana perusahaan untuk menghindari ancaman baru yang tidak terduga yang muncul di waktu yang akan datang.

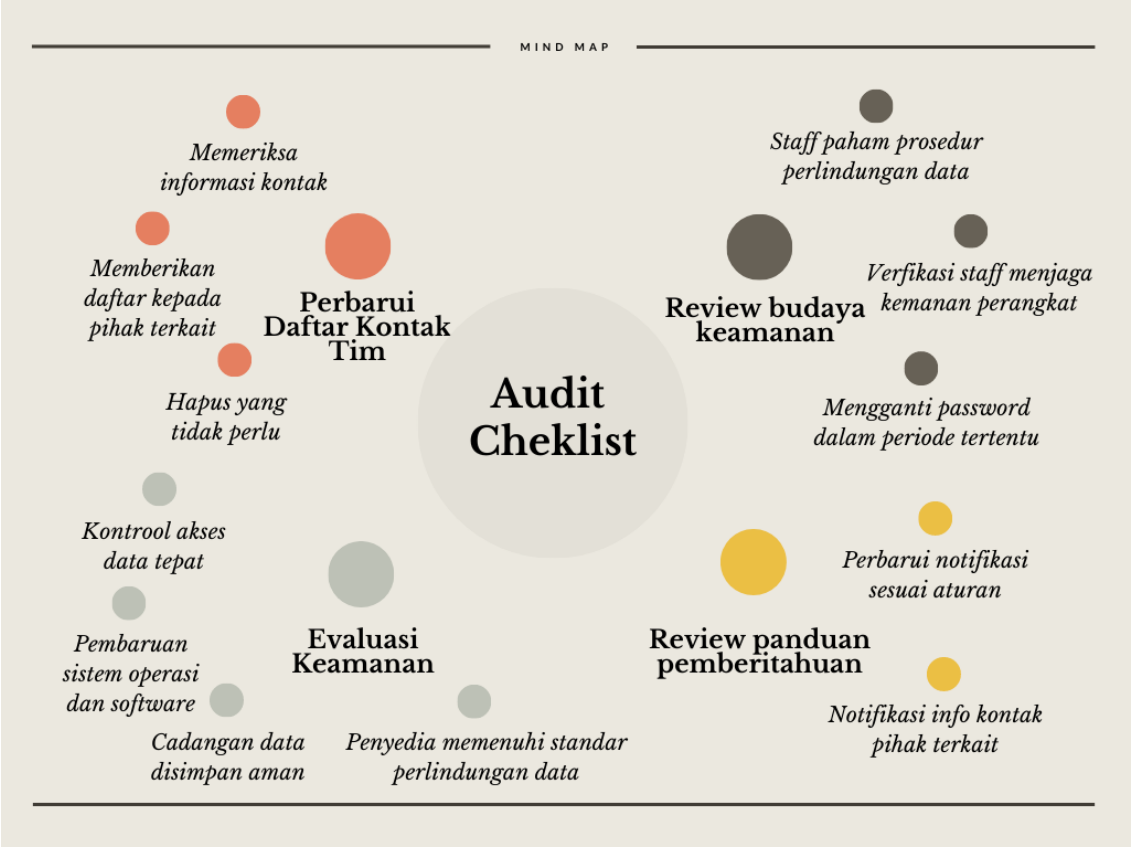
1. Fokus Area

Berikut ini adalah beberapa area yang dilaksanakan audit, yaitu :



2. Audit Checklist

Berikut ini adalah langkah yang dilakukan pada saat audit sesuai ruang lingkup respon perusahaan, yaitu :


MIND MAP
Audit Cheklist
Memeriksa informasi kontak
Memberikan daftar kepada pihak terkait
Perbarui Daftar Kontak Tim
Hapus yang tidak perlu
Kontrool akses data tepat
Pembaruan sistem operasi dan software
Evaluasi Keamanan
Cadangan data disimpan aman
Penyedia memenuhi standar perlindungan data
Staff paham prosedur perlindungan data
Review budaya keamanan
Verfikasi staff menjaga kemanan perangkat
Mengganti password dalam periode tertentu
Perbarui notifikasi sesuai aturan
Review panduan pemberitahuan
Notifikasi info kontak pihak terkait

REKOMENDASI

a. Memberikan tim Pusat Operasi Keamanan (SOC) dengan akses ke intelijen ancaman terbaru dan mendapatkan informasi terkini tentang alat, teknik serta taktik baru dan terkini yang digunakan oleh aktor ancaman dan pelaku *cyber crime*.
b. Mengimplementasikan solusi EDR untuk mendeteksi level *endpoint*, investigasi, dan remediasi insiden secara tepat waktu.
c. Selain mengadopsi perlindungan *endpoint* yang penting, juga perlu menerapkan solusi keamanan tingkat perusahaan yang mendeteksi ancaman lanjutan di tingkat jaringan pada tahap awal.
d. Menerapkan pelatihan dan kegiatan yang mengedukasi karyawan tentang dasar-dasar keamanan *cyber*, misalnya tidak membuka atau menyimpan file dari email atau situs web yang tidak dikenal karena dapat membahayakan seluruh perusahaan.
e. Secara berkala mengingatkan staf bagaimana menangani data sensitif, misalnya hanya menyimpan layanan cloud terpercaya dengan otentikasi diaktifkan, tidak membaginya kepada pihak ketiga yang tidak dipercaya.
f. Memiliki cadangan data penting dan melakukan pembaruan peralatan dan aplikasi TI secara teratur untuk menghindari kerentanan yang tidak tertandingi yang dapat menjadi alasan terjadinya pelanggaran.
g. Menggunakan produk *endpoint* khusus yang menuntut manajemen minimum yang memungkinkan karyawan untuk melakukan pekerjaan utama mereka namun tetap terlindung dari malware, ransomware, pengambilalihan akun, penipuan online, dan penipuan.

REFERENSI

[1] AllClear ID: "Data Breach Incident Response Workbook" https://dpoacademy.gr/_files/20000003-ba715bc634/ACID_Self_Service_Incident_Response_Workbook.pdf

[2] Experian: "Data Breach Response Guide" https://www.experian.com/assets/data-breach/brochures/response-guide.pdf

[3] https://id.wikipedia.org/wiki/Ilham_Bintang#:~:text=H.%20Ilham%20Bintang%20(lahir%20di,televisi%20di%20stasiun%20televisi%20swasta

[4] https://megapolitan.kompas.com/read/2020/02/05/13355011/kronologi-dan-peran-8-pelaku-pembobolan-rekening-ilham-bintang?page=all

[5] Panduan Menghadapi Data Breach, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas), Badan Siber dan Sandi Negara (BSSN)

2021 Microsoft Exchange Server Data Breach

Latar Belakang

Serangan dunia maya dan pelanggaran data dimulai pada Januari 2021, setelah melalui empat ekspliotasi di temukan server Microsoft Exchange Lokal. Yang memberikan penyerang akses penuh ke email dan kata sandi pengguna di server yang terpengaruh, hak istimewa administrator di server, dan akses ke perangkat yang terhubung di jaringan yang sama. Penyerangan biasa nya dilakukan melalui pintu belakang yang memungkinkan penyerang mengakses penuh ke server yang terkena dampak bahkan jika nanti server di perbaharui agar tidak lagi rentan terhadap eksploitasi. Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF)

Microsoft exchange dianggap sebagai target bernilai tinggi bagi peretas yang ingin menembus jaringan bisnis, karena ini adalah perangkat lunak server email, dan menurut microsoft ini menyediakan lingkungan unik yang memungkinkan penyerang melakukan berbagai tugas menggunakan perangkat bawaan yang sama.

Pada 5 Januari 2021, perusahaan penguji keamanan DEVCORE membuat laporan paling awal tentang kerentanan ke Microsoft, yang diverifikasi Microsoft pada 8 Januari. Pelanggaran pertama dari instans Microsoft Exchange Server diamati oleh perusahaan keamanan siber Volexity pada 6 Januari 2021. Pada akhir Januari, perusahaan keamanan siber Volexity telah mengamati pelanggaran yang memungkinkan penyerang untuk memata-matai dua pelanggan mereka, dan memberi tahu Microsoft tentang kerentanan. Setelah Microsoft diberi tahu tentang pelanggaran tersebut, Volexity mencatat bahwa peretas menjadi tidak terlalu sembunyi-sembunyi untuk mengantisipasi adanya tambalan.

Pada 2 Maret 2021, perusahaan keamanan siber lain, ESET , menulis bahwa mereka mengamati beberapa penyerang selain Hafnium yang mengeksploitasi kerentanan. Wired melaporkan pada 10 Maret bahwa sekarang setelah kerentanan telah ditambal, lebih banyak penyerang akan merekayasa balik perbaikan tersebut untuk mengeksploitasi server yang masih rentan. Analis di dua perusahaan keamanan melaporkan mereka mulai melihat bukti bahwa penyerang sedang bersiap untuk menjalankan perangkat lunak cryptomining di server.

Pada 10 Maret 2021, peneliti keamanan Nguyen Jang memposting kode bukti konsep ke GitHub milik Microsoft tentang cara kerja exploit, dengan total 169 baris kode; Program ini sengaja ditulis dengan kesalahan sehingga sementara peneliti keamanan dapat memahami cara kerja eksploitasi, pelaku jahat tidak akan dapat menggunakan kode tersebut untuk mengakses server. Kemudian pada hari itu, GitHub menghapus kode tersebut karena "berisi bukti kode konsep untuk kerentanan yang baru-baru ini diungkapkan yang sedang dieksploitasi secara aktif". Pada tanggal 13 Maret, grup lain secara independen menerbitkan kode eksploitasi, dengan kode ini memerlukan modifikasi minimal untuk bekerja; yang Koordinasi Pusat CERTWill Dormann mengatakan "eksploitasi benar-benar keluar dari kantong sekarang" sebagai tanggapan.

Serangan itu terjadi tak lama setelah pelanggaran data pemerintah federal Amerika Serikat tahun 2020 , yang juga menyebabkan aplikasi web dan rantai pasokan Microsoft Outlook dikompromikan . Microsoft mengatakan tidak ada hubungan antara kedua insiden tersebut.

Tujuan

Microsoft mengidentifikasi Hafnium sebagai "aktor yang sangat terampil dan canggih" yang secara historis sebagian besar menargetkan "entitas di Amerika Serikat untuk tujuan mengekstrak

informasi dari sejumlah sektor industri, termasuk peneliti penyakit menular, firma hukum, lembaga pendidikan tinggi , kontraktor pertahanan, lembaga pemikir kebijakan, dan LSM. " Mengumumkan peretasan tersebut, Microsoft menyatakan bahwa ini adalah "kali kedelapan dalam 12 bulan terakhir ini Microsoft telah secara terbuka mengungkapkan kelompok negara-bangsa yang menargetkan lembaga yang penting bagi masyarakat sipil." Pada 12 Maret 2021, ada, selain Hafnium, setidaknya sembilan kelompok berbeda lainnya yang mengeksploitasi kerentanan, masing-masing dengan gaya dan prosedur berbeda.

Kerugian

Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF).

wakil presiden Microsoft untuk Keamanan & Kepercayaan Pelanggan, menulis bahwa target mencakup peneliti penyakit, kantor hukum, universitas, kontraktor pertahanan, organisasi non-pemerintah , dan lembaga pemikir .

Check Point Research telah mengamati Amerika Serikat sebagai negara yang paling banyak diserang dengan 17% dari semua upaya eksploitasi, diikuti oleh Jerman dengan 6%, Inggris dan Belanda keduanya di 5%, dan Rusia dengan 4% dari semua eksploitasi; pemerintah / militer adalah sektor yang paling ditargetkan dengan 23% upaya eksploitasi, diikuti oleh manufaktur sebesar 15%, layanan perbankan dan keuangan sebesar 14%, vendor perangkat lunak dengan 7% dan perawatan kesehatan sebesar 6%

Pada 12 Maret 2021, Intelijen Keamanan Microsoft mengumumkan "keluarga baru ransomware " yang disebut DearCry sedang disebarkan ke server yang awalnya terinfeksi, mengenkripsi konten perangkat, membuat server tidak dapat digunakan, dan menuntut pembayaran untuk memulihkan file. Pada 18 Maret 2021, afiliasi ransomware cybergang REvil mengklaim bahwa mereka telah mencuri data tidak terenkripsi dari perusahaan perangkat keras dan elektronik Taiwan Acer , termasuk sejumlah perangkat yang dirahasiakan yang sedang dienkripsi, dengan firma keamanan siber Advanced Intel menautkan pelanggaran data ini dan serangan ransomware ke Microsoft Exchange eksploitasi.

Kesimpulan dan Saran Pengamanan

Pada 2 Maret 2021, Pusat Respons Keamanan Microsoft (MSRC) secara publik memposting rilis Common Vulnerabilities and Exposures (CVE) out-of-band , mendesak kliennya untuk menambal server Exchange mereka untuk mengatasi sejumlah kerentanan kritis . Pada tanggal 15 Maret, Microsoft merilis alat PowerShell sekali klik , Alat Mitigasi Exchange On-Premises, yang menginstal pembaruan spesifik yang melindungi dari ancaman, menjalankan pemindaian malware yang juga mendeteksi shell web yang diinstal, dan menghapus ancaman yang terdeteksi; ini direkomendasikan sebagai tindakan mitigasi sementara, karena tidak menginstal pembaruan lain yang tersedia.

Pada 3 Maret 2021, Cybersecurity and Infrastructure Security Agency (CISA) AS mengeluarkan arahan darurat yang memaksa jaringan pemerintah untuk memperbarui ke versi Exchange yang ditambal. Pada 8 Maret, CISA men-tweet apa yang NBC News gambarkan sebagai "pesan yang tidak biasa" mendesak "SEMUA organisasi di SEMUA sektor" untuk mengatasi kerentanan.

Badan resmi lainnya yang mengungkapkan keprihatinan termasuk Gedung Putih , Otoritas Keamanan Nasional Norwegia, dan Kantor Keamanan Cyber dan Informasi Republik Ceko. Pada 7 Maret 2021, CNN melaporkan bahwa pemerintahan Biden diharapkan membentuk satuan tugas untuk mengatasi pelanggaran tersebut; pemerintahan Biden telah mengundang organisasi sektor swasta untuk berpartisipasi dalam gugus tugas dan akan memberi mereka informasi rahasia yang dianggap perlu. Penasihat Keamanan Nasional AS Jake Sullivan menyatakan bahwa AS belum dalam posisi untuk disalahkan atas serangan itu.

2021 Microsoft Exchange Server Data Breach

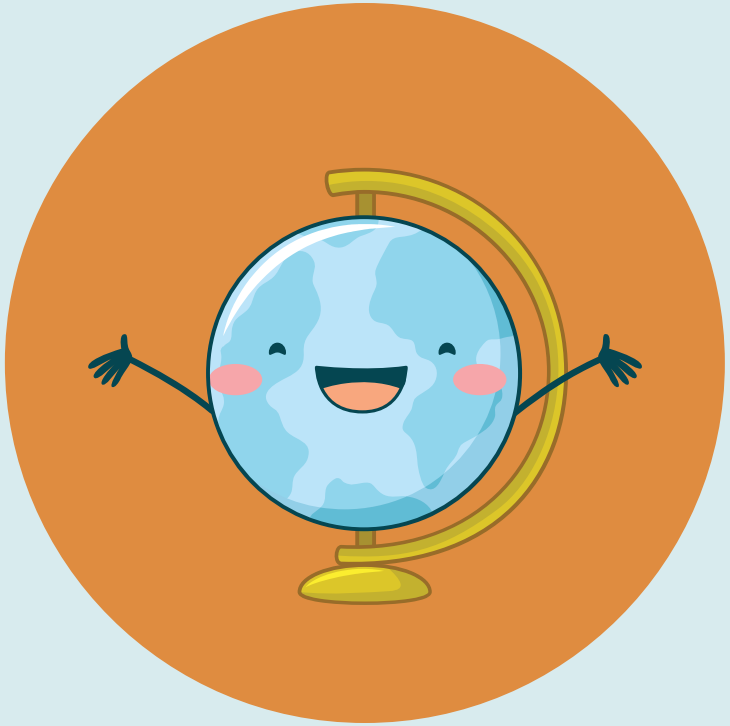
Nama

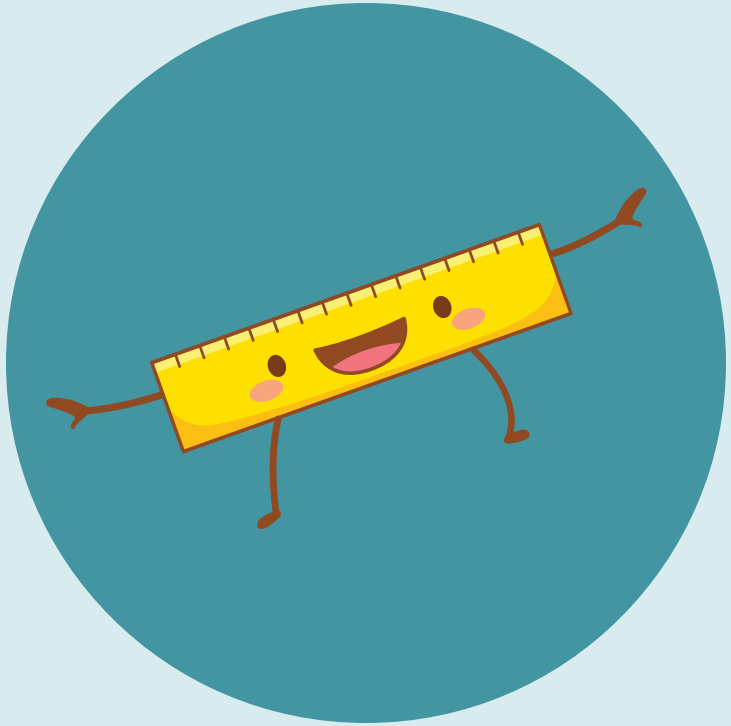
1.

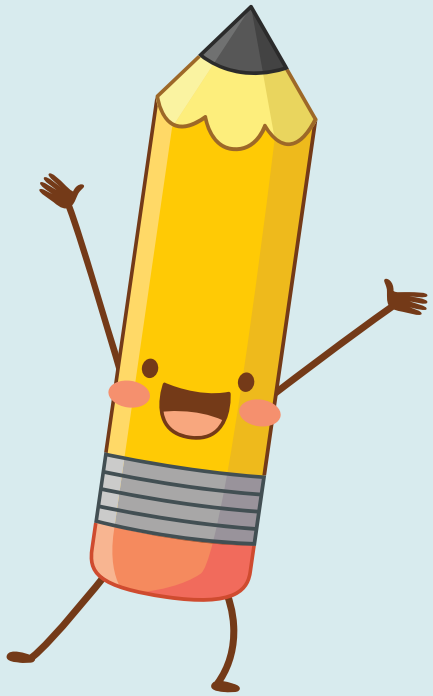
Latar Belakang

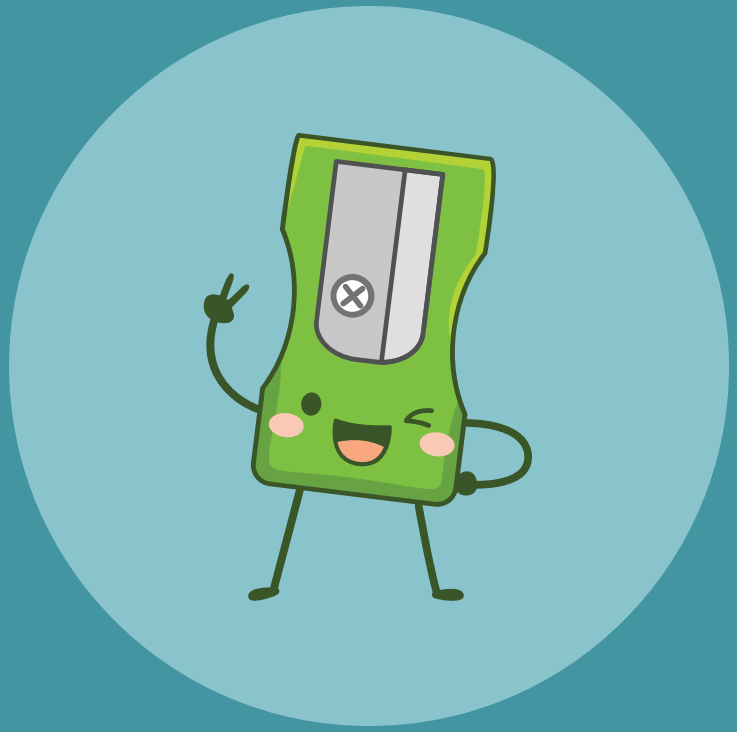
Tujuan

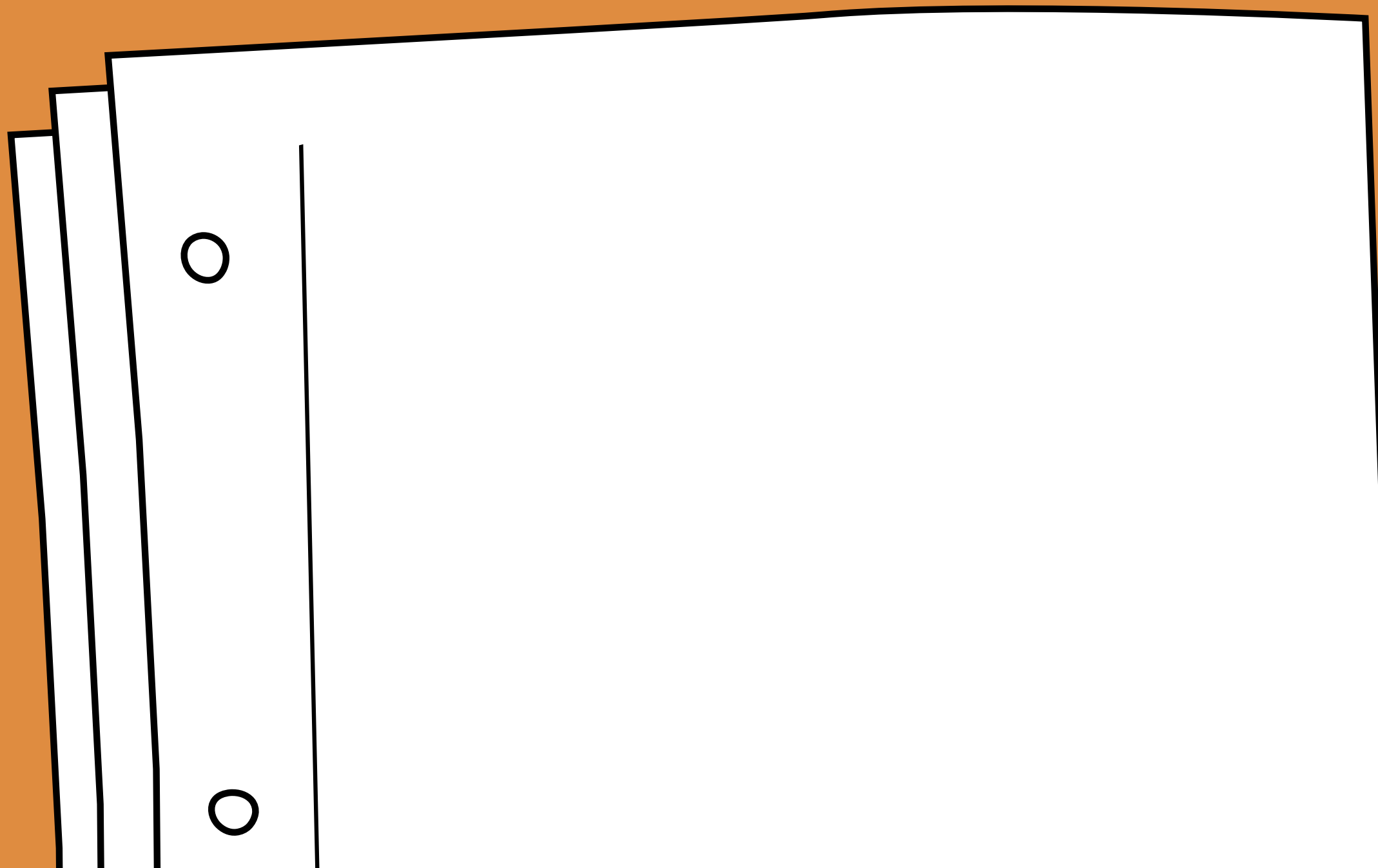
Kesimpulan & Saran











2021 Microsoft Exchange Server Data Breach

TUGAS IT AUDIT

OLEH :

NANDA S.PRAWIRA	**192420056**
RAHMI	**192420046**
RANI OKTA FELANI	**192420048**

PROGRAM PASCASARJANA

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

PALEMBANG

2020

2021 Microsoft Exchange Server Data Breach

Latar Belakang

Serangan dunia maya dan pelanggaran data dimulai pada Januari 2021, setelah melalui empat ekspliotasi di temukan server Microsoft Exchange Lokal. Yang memberikan penyerang akses penuh ke email dan kata sandi pengguna di server yang terpengaruh, hak istimewa administrator di server, dan akses ke perangkat yang terhubung di jaringan yang sama. Penyerangan biasa nya dilakukan melalui pintu belakang yang memungkinkan penyerang mengakses penuh ke server yang terkena dampak bahkan jika nanti server di perbaharui agar tidak lagi rentan terhadap eksploitasi. Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF)

Microsoft exchange dianggap sebagai target bernilai tinggi bagi peretas yang ingin menembus jaringan bisnis, karena ini adalah perangkat lunak server email, dan menurut microsoft ini menyediakan lingkungan unik yang memungkinkan penyerang melakukan berbagai tugas menggunakan perangkat bawaan yang sama.

Pada 5 Januari 2021, perusahaan penguji keamanan DEVCORE membuat laporan paling awal tentang kerentanan ke Microsoft, yang diverifikasi Microsoft pada 8 Januari. Pelanggaran pertama dari instans Microsoft Exchange Server diamati oleh perusahaan keamanan siber Volexity pada 6 Januari 2021. Pada akhir Januari, perusahaan keamanan siber Volexity telah mengamati pelanggaran yang memungkinkan penyerang untuk memata-matai dua pelanggan mereka, dan memberi tahu Microsoft tentang kerentanan. Setelah Microsoft diberi tahu tentang pelanggaran tersebut, Volexity mencatat bahwa peretas menjadi tidak terlalu sembunyi-sembunyi untuk mengantisipasi adanya tambalan.

Pada 2 Maret 2021, perusahaan keamanan siber lain, ESET , menulis bahwa mereka mengamati beberapa penyerang selain Hafnium yang mengeksploitasi kerentanan. Wired melaporkan pada 10 Maret bahwa sekarang setelah kerentanan telah ditambal, lebih banyak penyerang akan merekayasa balik perbaikan tersebut untuk mengeksploitasi server yang masih rentan. Analis di dua perusahaan keamanan melaporkan mereka mulai melihat bukti bahwa penyerang sedang bersiap untuk menjalankan perangkat lunak cryptomining di server.

Pada 10 Maret 2021, peneliti keamanan Nguyen Jang memposting kode bukti konsep ke GitHub milik Microsoft tentang cara kerja exploit, dengan total 169 baris kode; Program ini sengaja ditulis dengan kesalahan sehingga sementara peneliti keamanan dapat memahami cara kerja eksploitasi, pelaku jahat tidak akan dapat menggunakan kode tersebut untuk mengakses server. Kemudian pada hari itu, GitHub menghapus kode tersebut karena "berisi bukti kode konsep untuk kerentanan yang baru-baru ini diungkapkan yang sedang dieksploitasi secara aktif". Pada tanggal 13 Maret, grup lain secara independen menerbitkan kode eksploitasi, dengan kode ini memerlukan modifikasi minimal untuk bekerja; yang Koordinasi Pusat CERTWill Dormann mengatakan "eksploitasi benar-benar keluar dari kantong sekarang" sebagai tanggapan.

Serangan itu terjadi tak lama setelah pelanggaran data pemerintah federal Amerika Serikat tahun 2020 , yang juga menyebabkan aplikasi web dan rantai pasokan Microsoft Outlook dikompromikan . Microsoft mengatakan tidak ada hubungan antara kedua insiden tersebut.

Tujuan

Microsoft mengidentifikasi Hafnium sebagai "aktor yang sangat terampil dan canggih" yang secara historis sebagian besar menargetkan "entitas di Amerika Serikat untuk tujuan mengekstrak

informasi dari sejumlah sektor industri, termasuk peneliti penyakit menular, firma hukum, lembaga pendidikan tinggi , kontraktor pertahanan, lembaga pemikir kebijakan, dan LSM. " Mengumumkan peretasan tersebut, Microsoft menyatakan bahwa ini adalah "kali kedelapan dalam 12 bulan terakhir ini Microsoft telah secara terbuka mengungkapkan kelompok negara-bangsa yang menargetkan lembaga yang penting bagi masyarakat sipil." Pada 12 Maret 2021, ada, selain Hafnium, setidaknya sembilan kelompok berbeda lainnya yang mengeksploitasi kerentanan, masing-masing dengan gaya dan prosedur berbeda.

Peretas mengambil keuntungan dari empat kerentanan zero-day yang terpisah untuk mengganggu Outlook Web Access (OWA) server Microsoft Exchange , memberi mereka akses ke seluruh server dan jaringan korban serta ke email dan undangan kalender, hanya di pertama-tama memerlukan alamat server, yang dapat ditargetkan secara langsung atau diperoleh dengan pemindaian massal untuk server yang rentan; penyerang kemudian menggunakan dua eksploitasi, yang pertama mengizinkan penyerang untuk terhubung ke server dan melakukan otentikasi palsu sebagai pengguna standar. Dengan itu, kerentanan kedua kemudian dapat dieksploitasi, meningkatkan akses pengguna tersebut ke hak administrator . Dua eksploitasi terakhir memungkinkan penyerang untuk mengunggah kode ke server di lokasi mana pun yang mereka inginkan, yang secara otomatis berjalan dengan hak administrator ini. Penyerang kemudian biasanya menggunakan ini untuk menginstal shell web , menyediakan pintu belakang ke server yang disusupi, yang memberikan akses berkelanjutan kepada peretas ke server selama kedua shell web tetap aktif dan server Exchange tetap aktif.

Kerugian

Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF).

wakil presiden Microsoft untuk Keamanan & Kepercayaan Pelanggan, menulis bahwa target mencakup peneliti penyakit, kantor hukum, universitas, kontraktor pertahanan, organisasi non-pemerintah , dan lembaga pemikir .

Check Point Research telah mengamati Amerika Serikat sebagai negara yang paling banyak diserang dengan 17% dari semua upaya eksploitasi, diikuti oleh Jerman dengan 6%, Inggris dan Belanda keduanya di 5%, dan Rusia dengan 4% dari semua eksploitasi; pemerintah / militer adalah sektor yang paling ditargetkan dengan 23% upaya eksploitasi, diikuti oleh manufaktur sebesar 15%, layanan perbankan dan keuangan sebesar 14%, vendor perangkat lunak dengan 7% dan perawatan kesehatan sebesar 6%

Pada 12 Maret 2021, Intelijen Keamanan Microsoft mengumumkan "keluarga baru ransomware " yang disebut DearCry sedang disebarkan ke server yang awalnya terinfeksi, mengenkripsi konten perangkat, membuat server tidak dapat digunakan, dan menuntut pembayaran untuk memulihkan file. Pada 18 Maret 2021, afiliasi ransomware cybergang REvil mengklaim bahwa mereka telah mencuri data tidak terenkripsi dari perusahaan perangkat keras dan elektronik Taiwan Acer , termasuk sejumlah perangkat yang dirahasiakan yang sedang dienkripsi, dengan firma keamanan siber Advanced Intel menautkan pelanggaran data ini dan serangan ransomware ke Microsoft Exchange eksploitasi.

Kesimpulan dan Saran Pengamanan

Pada 2 Maret 2021, Pusat Respons Keamanan Microsoft (MSRC) secara publik memposting rilis Common Vulnerabilities and Exposures (CVE) out-of-band , mendesak kliennya untuk menambal server Exchange mereka untuk mengatasi sejumlah kerentanan kritis . Pada tanggal 15 Maret, Microsoft merilis alat PowerShell sekali klik , Alat Mitigasi Exchange On-Premises, yang menginstal pembaruan spesifik yang melindungi dari ancaman, menjalankan pemindaian

malware yang juga mendeteksi shell web yang diinstal, dan menghapus ancaman yang terdeteksi; ini direkomendasikan sebagai tindakan mitigasi sementara, karena tidak menginstal pembaruan lain yang tersedia.

Pada 3 Maret 2021, Cybersecurity and Infrastructure Security Agency (CISA) AS mengeluarkan arahan darurat yang memaksa jaringan pemerintah untuk memperbarui ke versi Exchange yang ditambal. Pada 8 Maret, CISA men-tweet apa yang NBC News gambarkan sebagai "pesan yang tidak biasa" mendesak "SEMUA organisasi di SEMUA sektor" untuk mengatasi kerentanan.

Badan resmi lainnya yang mengungkapkan keprihatinan termasuk Gedung Putih , Otoritas Keamanan Nasional Norwegia, dan Kantor Keamanan Cyber dan Informasi Republik Ceko. Pada 7 Maret 2021, CNN melaporkan bahwa pemerintahan Biden diharapkan membentuk satuan tugas untuk mengatasi pelanggaran tersebut; pemerintahan Biden telah mengundang organisasi sektor swasta untuk berpartisipasi dalam gugus tugas dan akan memberi mereka informasi rahasia yang dianggap perlu. Penasihat Keamanan Nasional AS Jake Sullivan menyatakan bahwa AS belum dalam posisi untuk disalahkan atas serangan itu.

2021 Microsoft Exchange Server Data Breach

Nama Anggota Kelompok :
1. Nanda S. Prawira
2. Rahmi
3. Rani Okta Felani

Latar Belakang

Serangan dunia maya dan pelanggaran data dimulai pada Januari 2021, setelah melalui empat ekspliotasi di temukan server Microsoft Exchange Lokal. Yang memberikan penyerang akses penuh ke email dan kata sandi pengguna di server yang terpengaruh, hak istimewa administrator di server, dan akses ke perangkat yang terhubung di jaringan yang sama. Penyerangan biasa nya dilakukan melalui pintu belakang yang memungkinkan penyerang mengakses penuh ke server yang terkena dampak bahkan jika nanti server di perbaharui agar tidak lagi rentan terhadap eksploitasi. Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF).

Microsoft exchange dianggap sebagai target bernilai tinggi bagi peretas yang ingin menembus jaringan bisnis, karena ini adalah perangkat lunak server email, dan menurut microsoft ini menyediakan lingkungan unik yang memungkinkan penyerang melakukan berbagai tugas menggunakan perangkat bawaan yang sama.

Pada 5 Januari 2021, perusahaan penguji keamanan DEVCORE membuat laporan paling awal tentang kerentanan ke Microsoft, yang diverifikasi Microsoft pada 8 Januari. Pelanggaran pertama dari instans Microsoft Exchange Server diamati oleh perusahaan keamanan siber Volexity pada 6 Januari 2021. Pada akhir Januari, perusahaan keamanan siber Volexity telah mengamati pelanggaran yang memungkinkan penyerang untuk memata-matai dua pelanggan mereka, dan memberi tahu Microsoft tentang kerentanan. Setelah Microsoft diberi tahu tentang pelanggaran tersebut, Volexity mencatat bahwa peretas menjadi tidak terlalu sembunyi-sembunyi untuk mengantisipasi adanya tambalan.

Pada 2 Maret 2021, perusahaan keamanan siber lain, ESET , menulis bahwa mereka mengamati beberapa penyerang selain Hafnium yang mengeksploitasi kerentanan. Wired melaporkan pada 10 Maret bahwa sekarang setelah kerentanan telah ditambal, lebih banyak penyerang akan merekayasa balik perbaikan tersebut untuk mengeksploitasi server yang masih rentan. Analis di dua perusahaan keamanan melaporkan mereka mulai melihat bukti bahwa penyerang sedang bersiap untuk menjalankan perangkat lunak cryptomining di server.

Pada 10 Maret 2021, peneliti keamanan Nguyen Jang memposting kode bukti konsep ke GitHub milik Microsoft tentang cara kerja exploit, dengan total 169 baris kode; Program ini sengaja ditulis dengan kesalahan sehingga sementara peneliti keamanan dapat memahami cara kerja eksploitasi, pelaku jahat tidak akan dapat menggunakan kode tersebut untuk mengakses server. Kemudian pada hari itu, GitHub menghapus kode tersebut karena "berisi bukti kode konsep untuk kerentanan yang baru-baru ini diungkapkan yang sedang dieksploitasi secara aktif". Pada tanggal 13 Maret, grup lain secara independen menerbitkan kode eksploitasi, dengan kode ini memerlukan modifikasi minimal untuk bekerja; yang Koordinasi Pusat CERTWill Dormann mengatakan "eksploitasi benar-benar keluar dari kantong sekarang" sebagai tanggapan.

Serangan itu terjadi tak lama setelah pelanggaran data pemerintah federal Amerika Serikat tahun 2020 , yang juga menyebabkan aplikasi web dan rantai pasokan Microsoft Outlook dikompromikan . Microsoft mengatakan tidak ada hubungan antara kedua insiden tersebut.

Tujuan

Microsoft mengidentifikasi Hafnium sebagai "aktor yang sangat terampil dan canggih" yang secara historis sebagian besar menargetkan "entitas di Amerika Serikat untuk tujuan mengekstrak informasi dari sejumlah sektor industri, termasuk peneliti penyakit menular, firma hukum, lembaga pendidikan tinggi , kontraktor pertahanan, lembaga pemikir kebijakan, dan LSM. " Mengumumkan peretasan tersebut, Microsoft menyatakan bahwa ini adalah "kali kedelapan dalam 12 bulan terakhir ini Microsoft telah secara terbuka mengungkapkan kelompok negara-bangsa yang menargetkan lembaga yang penting bagi masyarakat sipil." Pada 12 Maret 2021, ada, selain Hafnium, setidaknya sembilan kelompok berbeda lainnya yang mengeksploitasi kerentanan, masing-masing dengan gaya dan prosedur berbeda.

Peretas mengambil keuntungan dari empat kerentanan zero-day yang terpisah untuk mengganggu Outlook Web Access (OWA) server Microsoft Exchange , memberi mereka akses ke seluruh server dan jaringan korban serta ke email dan undangan kalender, hanya di pertama-tama memerlukan alamat server, yang dapat ditargetkan secara langsung atau diperoleh dengan pemindaian massal untuk server yang rentan; penyerang kemudian menggunakan dua eksploitasi, yang pertama mengizinkan penyerang untuk terhubung ke server dan melakukan otentikasi palsu sebagai pengguna standar. Dengan itu, kerentanan kedua kemudian dapat dieksploitasi, meningkatkan akses pengguna tersebut ke hak administrator . Dua eksploitasi terakhir memungkinkan penyerang untuk mengunggah kode ke server di lokasi mana pun yang mereka inginkan, yang secara otomatis berjalan dengan hak administrator ini. Penyerang kemudian biasanya menggunakan ini untuk menginstal shell web , menyediakan pintu belakang ke server yang disusupi, yang memberikan akses berkelanjutan kepada peretas ke server selama kedua shell web tetap aktif dan server Exchange tetap aktif.

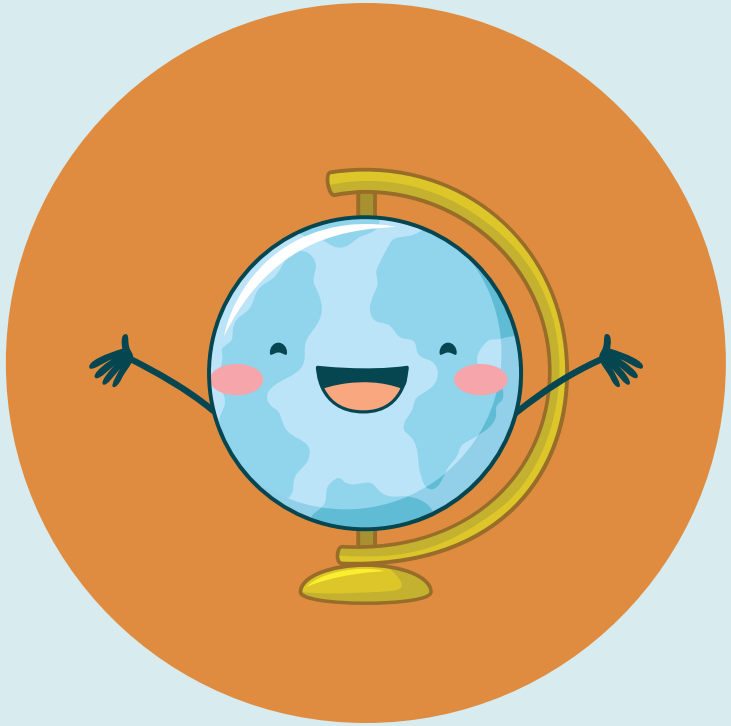
Kerugian

Per Maret 2021 di perkirakan 250.000 server menjadi korban serangan, termasuk server milik sekitar 30.000 organisasi di Amerika Serikat, 7000 server inggris serta otoritas perbankan eropa, parlemen norwegia, komisi cile untuk pasar keuangan (CMF).

wakil presiden Microsoft untuk Keamanan & Kepercayaan Pelanggan, menulis bahwa target mencakup peneliti penyakit, kantor hukum, universitas, kontraktor pertahanan, organisasi non-pemerintah , dan lembaga pemikir .

Check Point Research telah mengamati Amerika Serikat sebagai negara yang paling banyak diserang dengan 17% dari semua upaya eksploitasi, diikuti oleh Jerman dengan 6%, Inggris dan Belanda keduanya di 5%, dan Rusia dengan 4% dari semua eksploitasi; pemerintah / militer adalah sektor yang paling ditargetkan dengan 23% upaya eksploitasi, diikuti oleh manufaktur sebesar 15%, layanan perbankan dan keuangan sebesar 14%, vendor perangkat lunak dengan 7% dan perawatan kesehatan sebesar 6%

Pada 12 Maret 2021, Intelijen Keamanan Microsoft mengumumkan "keluarga baru ransomware " yang disebut DearCry sedang disebarkan ke server yang awalnya terinfeksi, mengenkripsi konten perangkat, membuat server tidak dapat digunakan, dan menuntut pembayaran untuk memulihkan file. Pada 18 Maret 2021, afiliasi ransomware cybergang REvil mengklaim bahwa mereka telah mencuri data tidak terenkripsi dari perusahaan perangkat keras dan elektronik Taiwan Acer , termasuk sejumlah perangkat yang dirahasiakan yang sedang dienkripsi, dengan firma keamanan siber Advanced Intel menautkan pelanggaran

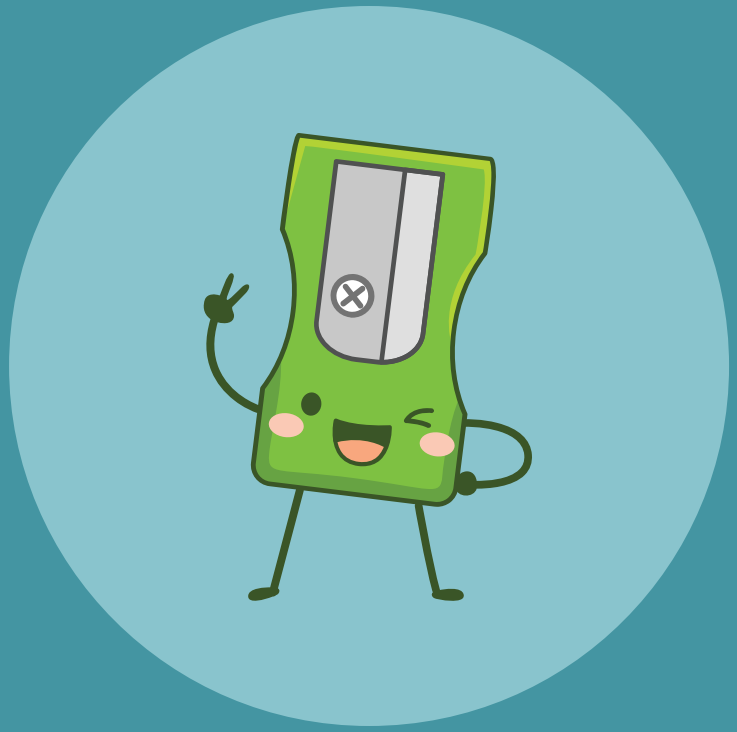


Kesimpulan & Saran

Pada 2 Maret 2021, Pusat Respons Keamanan Microsoft (MSRC) secara publik memposting rilis Common Vulnerabilities and Exposures (CVE) out-of-band , mendesak kliennya untuk menambal server Exchange mereka untuk mengatasi sejumlah kerentanan kritis . Pada tanggal 15 Maret, Microsoft merilis alat PowerShell sekali klik , Alat Mitigasi Exchange On-Premises, yang menginstal pembaruan spesifik yang melindungi dari ancaman, menjalankan pemindaian malware yang juga mendeteksi shell web yang diinstal, dan menghapus ancaman yang terdeteksi; ini direkomendasikan sebagai tindakan mitigasi sementara, karena tidak menginstal pembaruan lain yang tersedia.

Pada 3 Maret 2021, Cybersecurity and Infrastructure Security Agency (CISA) AS mengeluarkan arahan darurat yang memaksa jaringan pemerintah untuk memperbarui ke versi Exchange yang ditambal. Pada 8 Maret, CISA men-tweet apa yang NBC News gambarkan sebagai "pesan yang tidak biasa" mendesak "SEMUA organisasi di SEMUA sektor" untuk mengatasi kerentanan.

Badan resmi lainnya yang mengungkapkan keprihatinan termasuk Gedung Putih , Otoritas Keamanan Nasional Norwegia, dan Kantor Keamanan Cyber dan Informasi Republik Ceko. Pada 7 Maret 2021, CNN melaporkan bahwa pemerintahan Biden diharapkan membentuk satuan tugas untuk mengatasi pelanggaran tersebut; pemerintahan Biden telah mengundang organisasi sektor swasta untuk berpartisipasi dalam gugus tugas dan akan memberi mereka informasi rahasia yang dianggap perlu. Penasihat Keamanan Nasional AS Jake Sullivan menyatakan bahwa AS belum dalam posisi untuk disalahkan atas serangan itu.



TERIMAKASIH

ASSALAMMUALAIKUM ☺