



Legal Module

Practice Case 4
by: Dhea Fajriati Anas

How To Make Sure That The News Above Is TRUE (Not Hoax)?

PERIKSA SITUS DAN KUALITAS BERITA

Perhatikan sumber berita, apakah situs berita dapat dipercaya seperti situs resmi pemerintah, dan media resmi atau bersumber dari blogspot, broadcast grup chat atau situs yang asing terdengar.

Perhatikan penulisan berita, apakah ditulis sembarangan seperti banyak typo, tidak terstruktur, dan terlalu banyak pernyataan yang bersifat opini tanpa dasar data yang jelas.





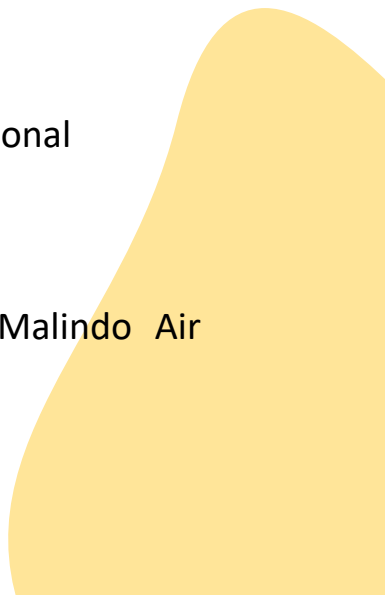
How To Make Sure That The News Above Is TRUE (Not Hoax)?

PERIKA SITUS DAN KUALITAS BERITA

Berita yang berjudul “**Lion Air Data Leak Came From Contractor's Ex-Staff, Airline Says**” adalah berita benar. Beberapa situs nasional dan internasional dengan berita serupa diantaranya,

- <https://www.ndtv.com/> : media televisi terbesar di India
- <https://www.scmp.com/> : surat kabar dari Hongkong
- <https://www.reuters.com/>: perusahaan berita dan informasi keuangan internasional
- <https://setkab.go.id/>: situs resmi Sekretariat Republik Indonesia
- <https://www.thejakartapost.com/>
- dll

Pernyataan yang ada pada berita berasal dari perusahaan maskapai yaitu, Malindo Air berdasarkan laporan dari Kaspersky Lab (perusahaan cybersecurity).



WHO WAS SUSPECTED TO STEAL THE CUSTOMER'S DATA?

Malindo Air memberikan pernyataan bahwa pelaku yang mencuri data konsumen adalah dua mantan pegawai penyedia layanan e-commerce GoQuo Sdn Bhd di pusat pengembangannya, India. Malindo Air tidak memberi tahu kepada publik nama dari kedua pelaku.

WHAT DATA COLUMNS WERE STOLEN? WERE THEY VIOLATING THE LAWS?

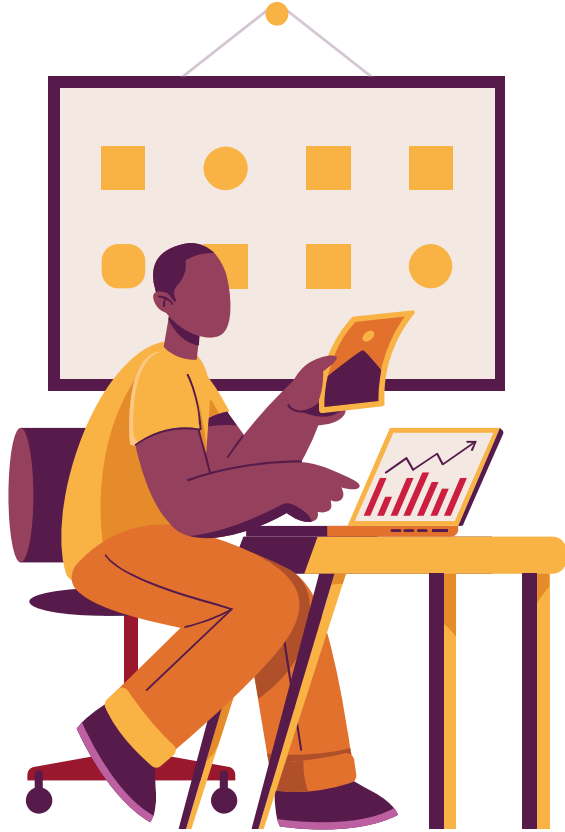
Data pribadi yang dicuri memiliki enam kolom yaitu, nama penumpang, alamat rumah, alamat email, tanggal lahir, nomor telepon, dan nomor paspor. Perilaku pencurian data pribadi merupakan suatu kegiatan ilegal sehingga dapat dikenakan sanksi pidana. Indonesia sendiri belum memiliki kebijakan atau regulasi terkait perlindungan data pribadi dalam satu undang-undang khusus, dan masih berupa rancangan.

Pada peraturan tingkat menteri, Menteri Komunikasi dan Informatika telah mengeluarkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi dalam Sistem Elektronik yang memuat ketentuan hak pemilik data pribadi, kewajiban pengguna data pribadi, kewajiban penyelenggara sistem elektronik, dan penyelesaian sengketa.





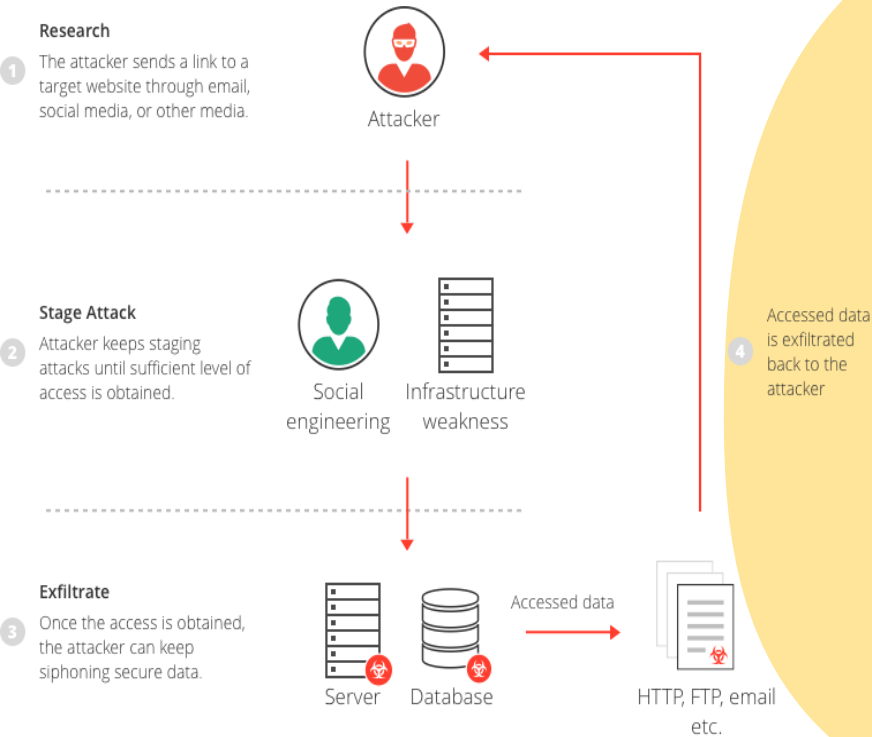
STRATEGIES TO PREVENT DATA BREACHES



DATA BREACH AND DATA LEAK DEFINITION

Data Breach atau Data Leak adalah pelepasan data sensitif, rahasia, atau terlindungi ke lingkungan yang tidak terpercaya. Pelanggaran data dapat terjadi sebagai akibat dari serangan peretas, pekerjaan orang dalam oleh individu yang saat ini atau sebelumnya dipekerjakan oleh suatu organisasi, atau kehilangan atau paparan data yang tidak disengaja. Akibatnya, data tersebut bisa hilang, atau digunakan oleh pelaku untuk berbagai tujuan jahat.

DATA BREACH CYCLE



- **Reconnaissance:** penyerang memulai dengan mengidentifikasi target potensial. Ini bisa berupa sistem TI, port atau protokol yang dapat diakses dan mudah ditembus atau dikompromikan.
- **Intrusion and presence:** penyerang melanggar perimeter keamanan organisasi.
- **Lateral movement and privilege escalation:** titik masuk penyerang mungkin tidak memungkinkan mereka untuk segera mendapatkan data sensitif. namun akan berusaha memperbaiki posisinya dengan pindah ke sistem dan akun pengguna lain. mereka memberikan akses ke data yang diinginkan.
- **Exfiltration:** penyerang mentransfer data sensitif ke luar jaringan organisasi, dan menggunakan data tersebut untuk keuntungan pribadi.

STRATEGIES TO PREVENT DATA BREACHES

1. Conduct Employee Security Awareness Training

Karyawan adalah mata rantai terlemah dalam rantai keamanan data suatu perusahaan seperti contohnya membuka e-mail mencurigakan dan tidak sengaja mengunduh virus. Pelatihan tentang siber dirasa perlu dilakukan lebih dari sekali untuk memberikan pengetahuan dan menumbuhkan kesadaran akan hal tersebut.



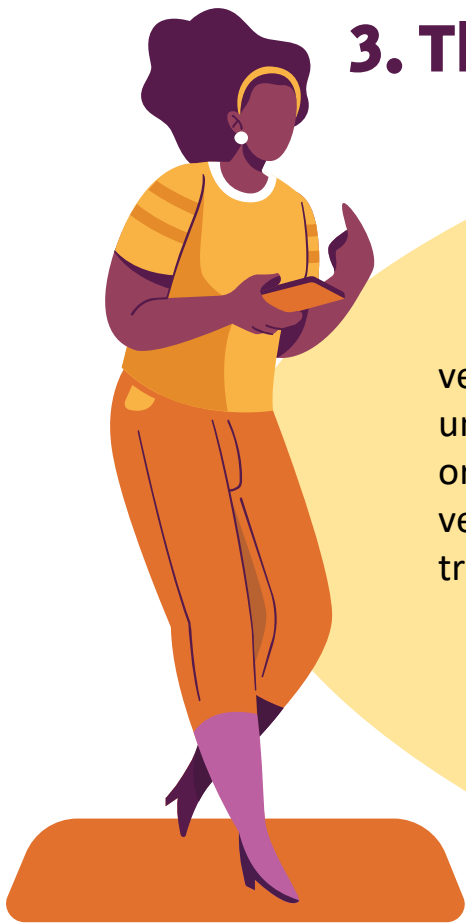
2. Limit Access To Most Valuable Data

Pada beberapa perusahaan, setiap karyawan memiliki akses ke semua file di komputer mereka. Hal tersebut tentu berbahaya sehingga membatasi akses perlu dilakukan. Saat pembatasan dilakukan tentu kita dapat mempersempit kumpulan karyawan yang mungkin secara tidak sengaja meng-klik tautan berbahaya. File tertentu sebaiknya hanya boleh diakses oleh mereka yang secara khusus membutuhkannya.



3. Third-Party Vendors Must Comply

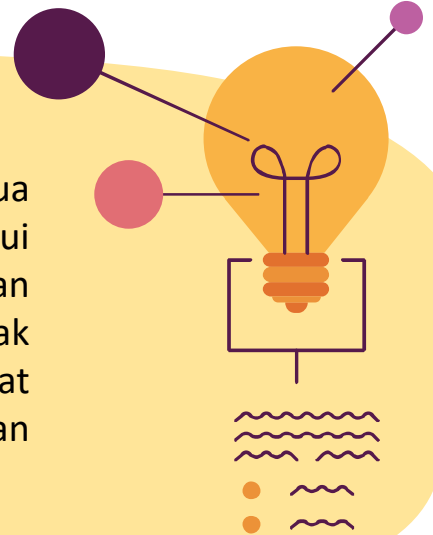
Setiap perusahaan melakukan bisnis dengan beragam vendor pihak ketiga. Sangatlah penting bagi perusahaan untuk mengenal siapa dan bagaimana latar belakang orang-orang yang terlibat di perusahaan vendor. Perusahaan vendor yang diizinkan untuk melihat data penting harus transparan terkait kepatuhan undang-undang privasi.



4. Update Software Regularly

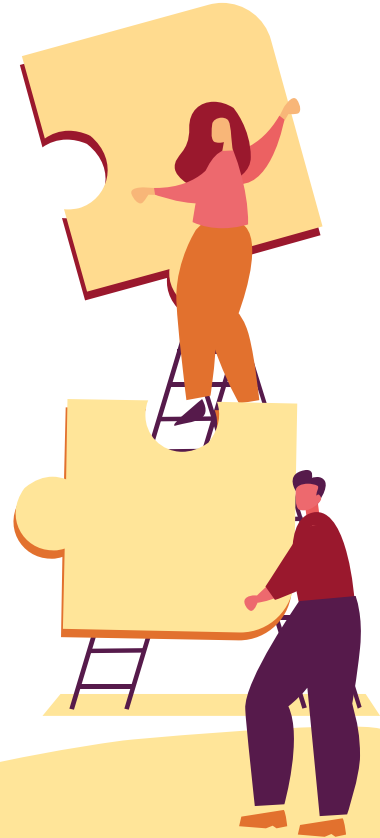


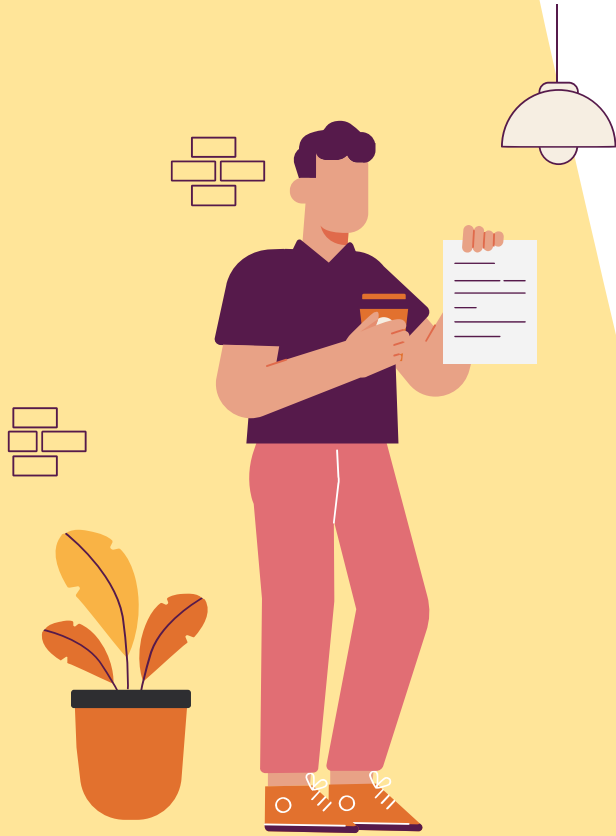
Para profesional menyarankan agar semua perangkat lunak aplikasi dan sistem operasi diperbarui secara berkala dengan melakukan instal patches kapan pun tersedia. Jaringan akan rentan ketika program tidak diperbarui secara berkala. Hal tersebut dapat memperkuat jaringan dan menghentikan serangan sebelum terjadi.



5. Develop A Cyber Breach Response Plan

Tidak ada yang tahu kapan pelanggaran akan terjadi. Perencanaan pelanggaran siber yang komprehensif tentu diperlukan untuk memahami potensi kerusakannya. Rencana respons bisa dimulai dengan evaluasi apa yang hilang dan kapan, bahkan siapa yang berpotensi untuk bertanggungjawab. Jika perencanaan pelanggaran dilakukan, perusahaan dapat bertindak secara cepat dan tegas sehingga dapat membatasi kerusakan dan memulihkan kepercayaan publik dan karyawan.





Thanks!

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

Daftar Pustaka



<https://www.imperva.com/learn/data-security/data-breach/>

<https://www.techsupportofmn.com/6-ways-to-prevent-cybersecurity-breaches>

<https://www.gdpr.associates/data-breach-prevention/>

<https://paysimple.com/blog/how-to-prevent-data-breach/>

<https://hybrid.co.id/amp/post/kebocoran-data-harus-jadi-perhatian-sejak-awal>

