Incident report analysis

Summary	Di pagi ini, seorang pegawai intern melaporkan kepada tim IT bahwa ia tidak dapat masuk ke akun jaringan internalnya. Namun, catatan akses menunjukkan aktivitas dari akun tersebut pada database pelanggan, meskipun aksesnya telah terkunci. Pegawai intern menjelaskan bahwa ia menerima email yang mengarahkan ke sebuah situs eksternal dan diminta login menggunakan kredensial internal untuk mengambil pesan. Kami menduga inilah cara penyerang memperoleh akses tidak sah ke sistem dan database pelanggan. Beberapa pegawai lain juga menemukan bahwa sejumlah data pelanggan hilang atau terisi informasi yang salah, sehingga kemungkinan besar data tidak hanya terekspos, tetapi juga dihapus maupun dimanipulasi.
Identify	Tim manajemen insiden melakukan audit terhadap perangkat, sistem, dan kebijakan akses yang terkait untuk menemukan celah keamanan. Dari hasil audit, diketahui bahwa kredensial intern berhasil dicuri dan dimanfaatkan penyerang untuk masuk ke database pelanggan. Pemeriksaan awal juga memperlihatkan bahwa sebagian data pelanggan telah dihapus.
Protect	Sebagai langkah pencegahan, tim menetapkan kebijakan autentikasi baru: penerapan autentikasi multi-faktor (MFA), pembatasan maksimal tiga kali percobaan login, serta pelatihan seluruh pegawai terkait perlindungan kredensial. Selain itu, konfigurasi firewall akan diperbarui dan perusahaan akan berinvestasi pada sistem pencegahan intrusi (IPS).
Detect	Untuk memperkuat deteksi dini, tim akan menggunakan fitur logging pada firewall dan mengimplementasikan sistem deteksi intrusi (IDS) guna memantau seluruh lalu lintas internet yang masuk.

Respond	Akun intern yang terdampak langsung dinonaktifkan. Seluruh karyawan, termasuk intern, diberi pelatihan mengenai keamanan kredensial. Pihak manajemen telah diberitahu, dan mereka akan mengirim pemberitahuan resmi kepada pelanggan terkait kebocoran data. Selain itu, manajemen juga berkewajiban melapor ke pihak berwenang sesuai ketentuan hukum setempat.
Recover	Tim akan mengembalikan data dengan melakukan restorasi database dari backup penuh yang dilakukan malam sebelumnya. Informasi pelanggan yang ditambahkan atau diubah pada pagi ini tidak akan tercatat, sehingga staf perlu memasukkan ulang data tersebut setelah proses pemulihan selesai.

Reflections/Notes:
Insiden ini memperlihatkan bahwa serangan phishing masih menjadi salah satu ancaman terbesar dalam keamanan siber perusahaan. Kasus yang menimpa seorang intern menunjukkan bahwa kurangnya kewaspadaan dan pengalaman dapat dimanfaatkan oleh pihak luar untuk memperoleh akses ilegal. Oleh karena itu, peningkatan kesadaran keamanan tidak cukup hanya dengan pelatihan satu kali, tetapi perlu ditunjang dengan simulasi dan uji coba berkala agar setiap pegawai mampu mengenali pola serangan serupa.

Selain itu, kebijakan autentikasi sebelumnya terbukti belum cukup kuat untuk mencegah penyalahgunaan akun. Implementasi multi-factor authentication (MFA) merupakan langkah penting yang harus segera dijalankan, disertai pembatasan percobaan login dan pengawasan ketat terhadap kredensial pegawai. Di sisi lain, kebutuhan akan sistem deteksi dan pencegahan intrusi juga semakin jelas, sebab monitoring real-time dapat mempercepat deteksi serta memungkinkan respon lebih dini sebelum kerugian semakin meluas.

Proses pemulihan data melalui backup menunjukkan betapa pentingnya strategi cadangan rutin. Walau demikian, keterbatasan backup harian yang tidak mencatat perubahan data terbaru menjadi catatan penting agar ke depan perusahaan dapat mempertimbangkan metode pemulihan yang lebih adaptif.

Akhirnya, komunikasi yang cepat dan terbuka antara tim IT, manajemen, pegawai, serta pelanggan menjadi faktor kunci dalam menjaga kepercayaan publik. Ke depan, organisasi harus melakukan evaluasi rutin terhadap kebijakan keamanan yang ada agar selalu sejalan dengan perkembangan ancaman siber yang terus berubah.