CERDAS
Cerita & **E**dukasi e**R**a **D**igital
Amankan **S**istem pembayaran

ASPI
Asosiasi Sistem Pembayaran Indonesia

CYBER HEIST

Di era digital yang berkembang pesat, keamanan data dan privasi pengguna menjadi tantangan utama dalam sistem pembayaran. Salah satu ancaman nyata dan terus berkembang ialah *Cyber Heist*, yakni pencurian atau peretasan yang dilakukan melalui sistem digital dan jaringan komputer dan berdampak terhadap pencurian data yang bisa mengarah kepada aktifitas transaksi fiktif (*fraud*) dalam sistim pembayaran.

Untuk itu, menjaga keamanan data dan melindungi privasi pengguna menjadi hal krusial, yang tidak hanya menjadi tanggung jawab Penyedia Jasa Pembayaran (PJP) dan Penyelenggara Infrastruktur Pembayaran (PIP), namun termasuk juga mitra PJP dan PIP yang memiliki peran penting dalam ekosistem sistem pembayaran nasional.

Terdapat tiga aspek proteksi terhadap serangan siber antara lain:

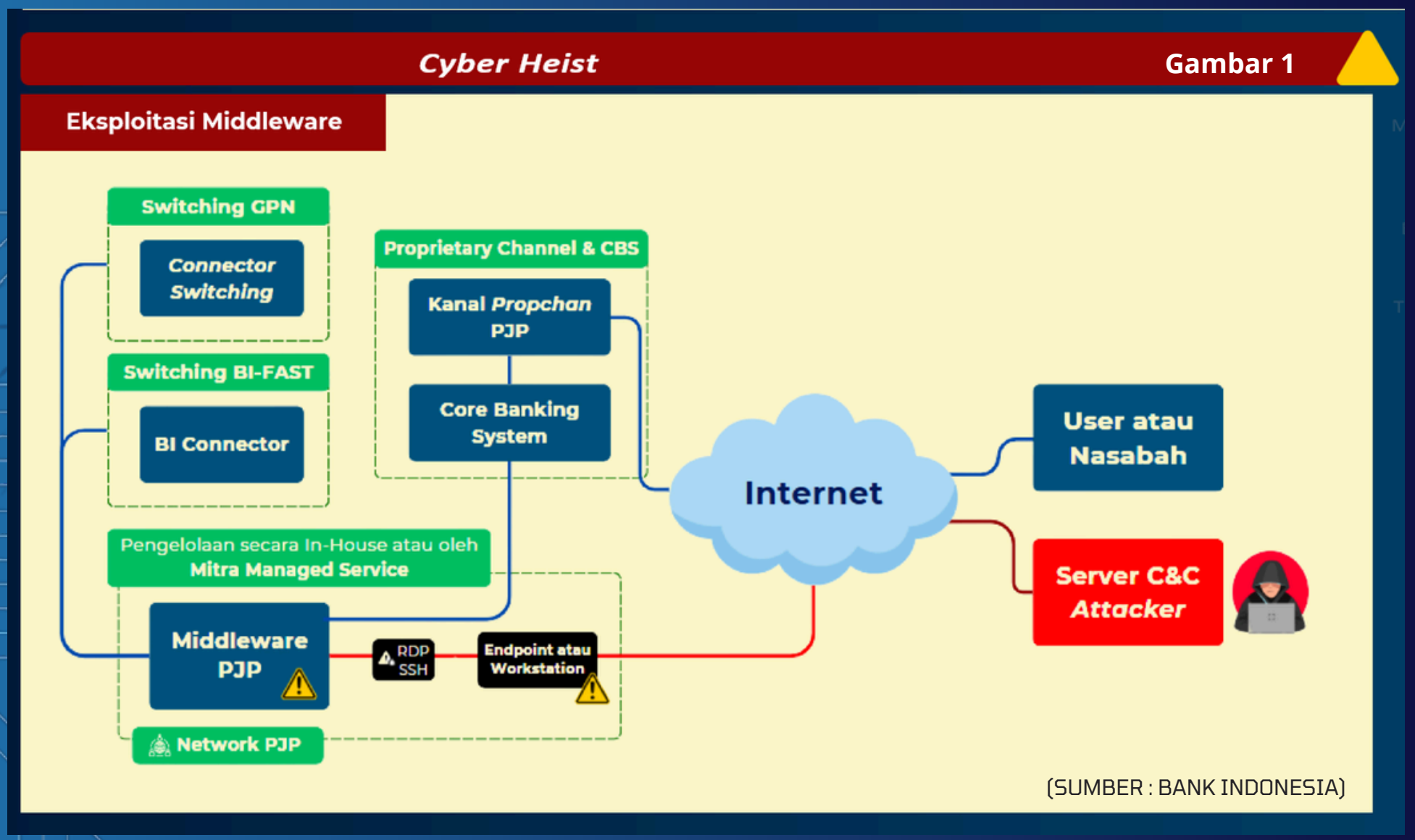
- ***People***, merupakan titik kelemahan paling dominan. Berdasarkan dari analisa Microsoft ***"Cybersecurty Red Team"*** yang berlaku di seluruh industri, mengidentifikasi bahwa saat ini *attacker* menyasar serangan terhadap individu yang ada dalam internal jaringan korporasi. Hal ini disebabkan karena aspek *people* merupakan titik paling rentan dan *entry point* yang paling mudah di eksploitasi oleh aktor serangan siber, ***"People is the weakest link in cybersecurity chain"***.

- ***Process***, merupakan salah satu kelemahan yang sangat umum, disebabkan tidak adanya aktivitas *Security Penetration Test* yang harus dijalankan secara rutin dan berkala minimal setiap 6 bulan sekali atau ketika dilakukan perubahan konfigurasi sistem infrastruktur dan coding aplikasi. *Governance* terhadap penanganan *password* sistem atau server krtikal yang tidak dilakukan mengikuti tata kelola yang benar dan tidak mengikuti standar *best practice* dengan menggunakan *tools privilege access management* (PAM).

- ***Technology***, merupkan hal umum terjadi dikarenakan adanya celah kerentanan terhadap *code* aplikasi *software* yang dikembangkan oleh para *software developer.* Kerentanan terhadap serangan siber juga bisa terjadi ketika tidak dilakukan *security patch update* secara regular.

Salah satu insiden Cyber Heist pada sistem pembayaran, menunjukkan attacker berhasil masuk ke dalam jaringan internal sistem middleware mitra PJP/PIP. Hasil digital forensik ditemukan bahwa serangan bermula dari adanya kerentanan atau kelemahan pelindungan pada perangkat pengguna karena tidak adanya anti malware yang memadai seperti mengadopsi teknologi XDR protection dan rendahnya kesadaran pengguna dalam serangan phishing dan social engineering.

Dampak yang sering terjadi adalah kredensial *user-id* dan *password* pada perangkat sudah ter-*compromise*. Sehingga memudahkan *attacker* mengambil alih kontrol perangkat tersebut untuk melakukan aktifitas *Command and Control (CNC)* secara *remote*. Selanjutnya *attacker* dengan mudah melakukan *lateral movement* dalam jaringan internal mitra PJP untuk mengakses sistem server yang memiliki *privilege* paling tinggi dengan tujuan melakukan aktivitas yang lebih desktruktif sampai dengan melakukan pencurian data dan menginstruksikan untuk melakukan aktifitas transaksi fiktif.



(SUMBER : BANK INDONESIA)

CERDAS

Cerita & **E**dukasi e**R**a **D**igital
Amankan **S**istem pembayaran

ASPI
Asosiasi Sistem Pembayaran Indonesia

Berikut kerentanan secara umum terhadap *Cyber Heist* yang harus menjadi perhatian dan dicegah:
1. Terbukanya protokol komunikasi yang tidak aman seperti *Remote Desktop Protokol (*RDP) tanpa adanya proteksi *protokol Secured Shell* (SSH) seperti yang diterapkan *cloudflare*, dimana kerentanan ini dapat membuka pintu akses kedalam internal jaringan tanpa adanya proteksi pengamanan jaringan yang memudahkan *attacker* me-*remote* akses kedalam kritikal server.

2. Tidak adanya proses validasi aksesibilitas jaringan VPN minimal dengan penerapan *two factor authentication* (2FA) yang berfungsi untuk memvalidasi apakah perangkat akses yang dipergunakan sudah sah dan terdaftar. Sebagai contoh *Token Code* yang banyak diterapkan di industri sistem pembayaran.

3. Diperlukan merubah aplikasi Web akses yang wajib menggunakan mekanisme enkripsi HTTPS.

4. Tidak adanya *tools Threat Detection System* secara yang berfungsi untuk mendeteksi potensi serangan siber dan melaporkan secara *real time bases*.

5. Masih banyak ditemukan perangkat dan piranti infrastruktur yang sudah *obsolet*e sehinga tidak memiliki *update security patch* yang memadai dan terkini.

6. Lemahnya pelaksanaan Audit TI dan/atau KKS, dimana pelaksanaan *penetration testing,* belum dilakukan secara indpenden dan menyeluruh di mulai dari *network infrastructure penetration test* hingga *application penetration testing.*

7. Masih terbukanya akses internet terhadap *critical infrastruktur* TI, sehingga membuka celah *attacker* melakukan CNC untuk meningkatkan aktifitas serangan siber secara remote. Ini memberikan kemudahan *attacker* memerintahkan *lateral movement* dalam internal jaringan untuk mendapatkan *privilage user* akses tertinggi, serta melakukan aktifitas *destruktif* sampai dengan aktifitas *fraud.*

Kerentanan	Risiko dan Dampak	Mitigasi yang Disarankan
Akses RDP tanpa SSH	Potensi terjadinya akses ilegal terhadap server kritikal yang dapat berimplikasi pada pencurian data konsumen maupun manipulasi sistem inti.	Menutup seluruh akses RDP publik, menerapkan SSH tunnel, serta memperkuat firewall dengan prinsip *least privilege*.
VPN tanpa MFA/2FA	Membuka peluang pencurian kredensial dan pengambilalihan akun internal yang dapat mengarah pada pembajakan akun berhak istimewa serta transaksi fiktif.	Penerapan otentikasi multi faktor, baik melalui token, OTP, maupun biometrik, untuk seluruh akses VPN.
Aplikasi Web tanpa HTTPS	Risiko terjadinya *data sniffing* dan kebocoran informasi sensitif selama proses transaksi, yang berdampak pada kerahasiaan data pribadi konsumen.	Penerapan enkripsi TLS 1.3 pada seluruh aplikasi serta penggunaan sertifikat digital yang valid dan terpercaya.
Ketiadaan Sistem Deteksi Ancaman	Serangan siber tidak teridentifikasi secara dini sehingga menimbulkan kerugian finansial signifikan serta eksposur data yang berkepanjangan.	Implementasi sistem SIEM, XDR, atau IDS/IPS dengan pemantauan 24/7 melalui *Security Operations Center* (SOC).
Infrastruktur Usang (Obsolete)	Kerentanan tinggi terhadap malware maupun ransomware akibat perangkat keras dan lunak yang tidak lagi mendapatkan pembaruan keamanan.	Program manajemen siklus hidup aset TI, termasuk pembaruan infrastruktur serta penerapan patch keamanan secara rutin.
Audit TI yang Lemah	Banyak celah keamanan tidak teridentifikasi sehingga menimbulkan risiko ketidakpatuhan terhadap ketentuan regulator serta eksposur ancaman yang tidak terkendali.	Pelaksanaan *penetration test* dan audit TI independen secara berkala.
Akses Internet ke Server Kritikal	Memberikan peluang bagi pelaku untuk melakukan *command and control* serta pengambilalihan penuh terhadap server kritikal, berujung pada pencurian data dan transaksi fiktif.	Penerapan segmentasi jaringan, arsitektur *Zero Trust*, serta penggunaan *bastion host* untuk mengendalikan akses ke sistem kritikal.

Sistem pembayaran digital tidak hanya dinilai dari aspek kecepatan dan efisiensi transaksi, dengan adanya perkembanagn berbagai modus *fraud* dan maraknya pencurian data, seluruh pelaku sistem pembayaran nasional wajib menetapkan keamanan pertukaran data sebagai prioritas utama yang perlu ditingkatkan seiring dengan berkembanngnya inovasi produk, layanan, dan solusi pembayaran digital.