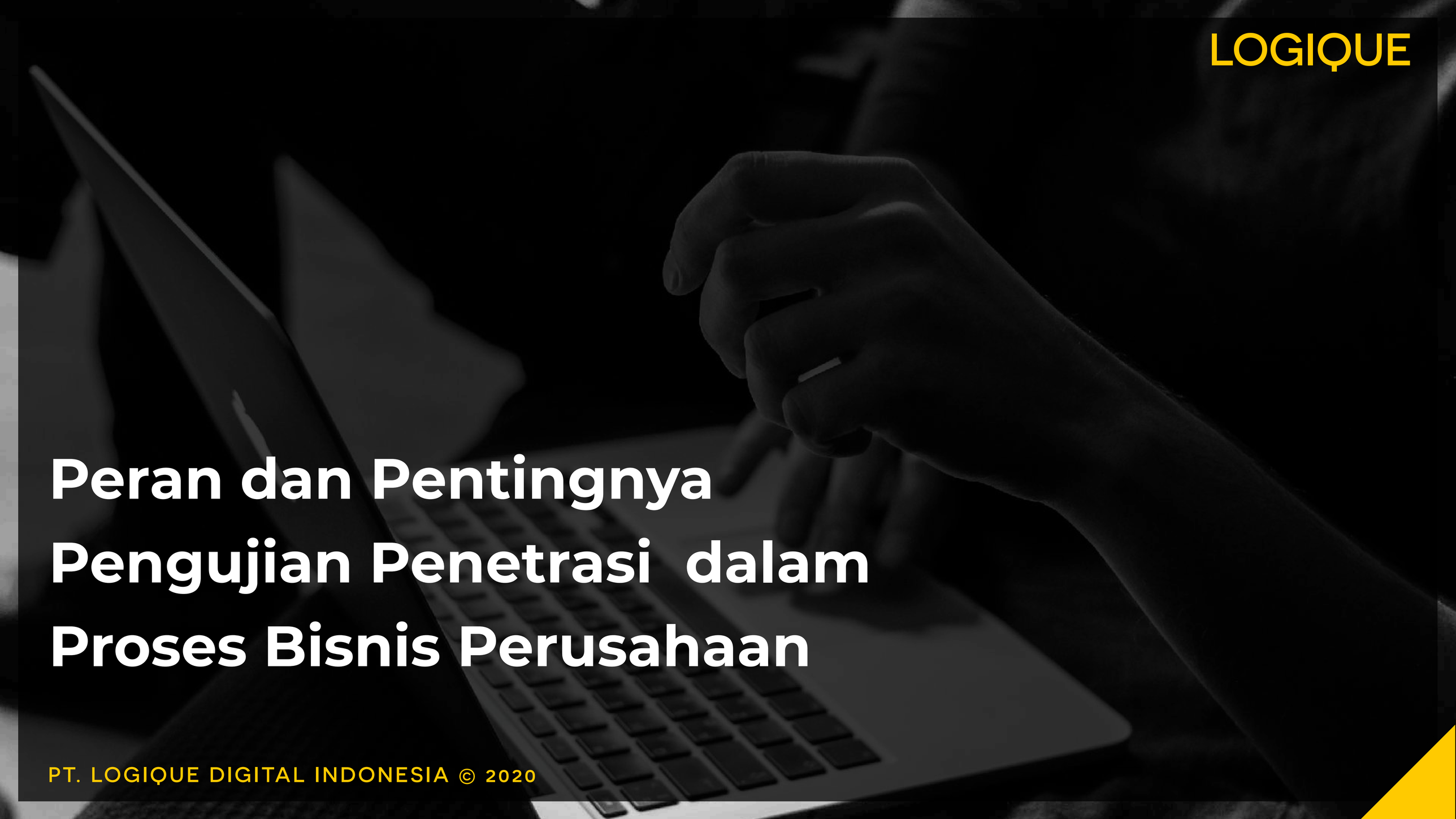


LOGIQUE

Peran dan Pentingnya Pengujian Penetrasi dalam Proses Bisnis Perusahaan

Intro.

Teknologi Informasi dan Internet telah banyak mengubah cara hidup bagi sebagian orang di Indonesia, bagaimana tidak banyak aktivitas sehari-hari dapat dimudahkan dengan teknologi informasi dan internet, hal ini tentu dapat meningkatkan terhadap kerentanan keamanan informasi terhadap sebuah organisasi dari risiko serangan cyber.

Berdasarkan data dari BSSN dalam rentang waktu anrata bulan Januari-April 2020 di Indonesia terjadi seragan sebanyak 88.414.296 serangan siber *(sumber: https://bssn.go.id/rekap-serangan-siber-januari-april-2020/)*. Angka tersebut menggambarkan betapa masifnya serangan yang terjadi, dengan demikian banyaknya angka serangan siber yang terjadi perlu menjadi perhatian khusus bagi seluruh pemangku kebijakan pada setiap organisasi.

Ancaman serangan siber bisa terjadi kapanpun dan di manapun, organisasi perusahaan bisa saja menjadi target para pelaku kejahatan siber, di mana keamanan informasi menjadi salah satu yang sangat penting. Berbicara mengenai keamanan informasi terdapat 3 aspek dasar yang harus diperhatikan yaitu adalah Confidentiality, Integrity dan Availability. Dalam prespektif bisnis ketiga aspek tersebut menjadi hal yang penting agar bisnis yang dijalankan oleh suatu perusahaan dapat berjalan dengan baik.

1. Confidentiality

Poin ini mencakup kerahasiaan yang berarti adalah suatu serangkaian upaya untuk menjaga suatu kerahasiaan suatu informasi atau data pada suatu organisasi

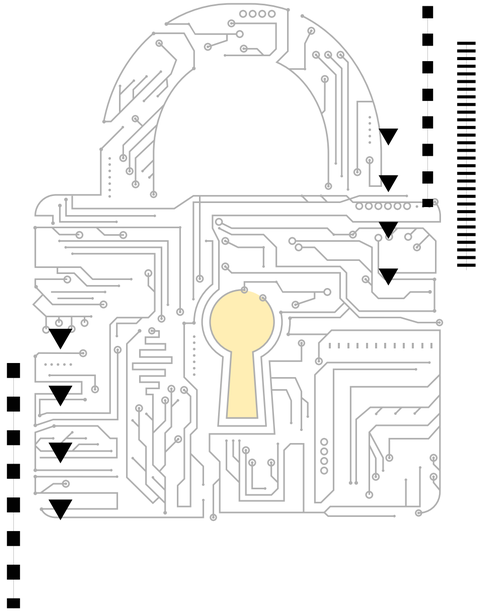
2. Integrity

Integritas data / informasi adalah hal yang penting, dalam hal ini adalah suatu metode untuk menjaga agar suatu data / informasi tidak dapat dimanipulasi, diubah atau diedit oleh pihak yang tidak punya wewenang

3. Availability

Ketersediaan suatu infrastruktur juga hal yang penting agar layanan bisnis dapat terus beroperasi, untuk itu dalam konteks keamanan informasi upaya menjaga sebuah sistem agar tetap terus bisa digunakan adalah hal yang perlu dilakukan.

Dalam suatu organisasi bisnis yang memanfaatkan teknologi informasi (IT) tentunya terdapat infrastruktur IT yang menopang bisnis tersebut agar bisnis pada suatu perusahaan terus tetap berjalan. Pengujian penetrasi terhadap infrastruktur IT penting dilakukan, hal ini bertujuan untuk mendapatkan peningkatan kualitas keamanan infrastrujtur IT pada suatu perusahaan baik itu web apps, mobile apps ataun network infrastrukturnya.



Pengujian penetrasi atau yang sering disebut Penetration Testing

adalah sebuah metode pengujian terhadap infrastruktur IT menggunakan cara-cara yang sering digunakan oleh *hackers* di dunia nyata. Seperti yang sudah disampaikan sebelumya terdapat 3 aspek dasar yang harus diperhatikan dalam keamanan informasi yaitu adalah Confidentiality, Integrity dan Availability, untuk itu Penetration Testing dilakukan untuk mencoba mengeksploitasi dan mengidentifikasi kerentanan tiga aspek tersebut. Selain itu Penetration testing juga bertujuan untuk memberikan saran dan solusi untuk perbaikan tentang bagaimana menguraangi risiko dan dampak yang terjadi apabila ketiga aspek kemanan informasi tersebut dapat dieksploitasi.

Mengapa harus melakukan Penetration Testing?

Banyaknya serangan siber yang terjadi tentunya akan meningkatkan ancaman siber pada suatu organisasi perusahaan, ancaman siber dapat mengganggu proses bisnis bahkan juga dapat mempengaruhi reputasi dari perusahaan tersebut. Untuk itu Penetration testing perlu dilakukan. **Mengapa?**

1. Identifikasi Kerentanan Lebih awal

Saat dilakukan pentest Anda akan dapat mengidentifikasi sebuah kerentanan dalam infrastrukture IT anda, hal ini akan membantu Anda untuk segera menutup dan memperbaiki celah pada infrastruktur Anda sedini mungkin sebelum “hacker” mengeksploitasinya.

2. Meningkatkan Kualitas Keamanan

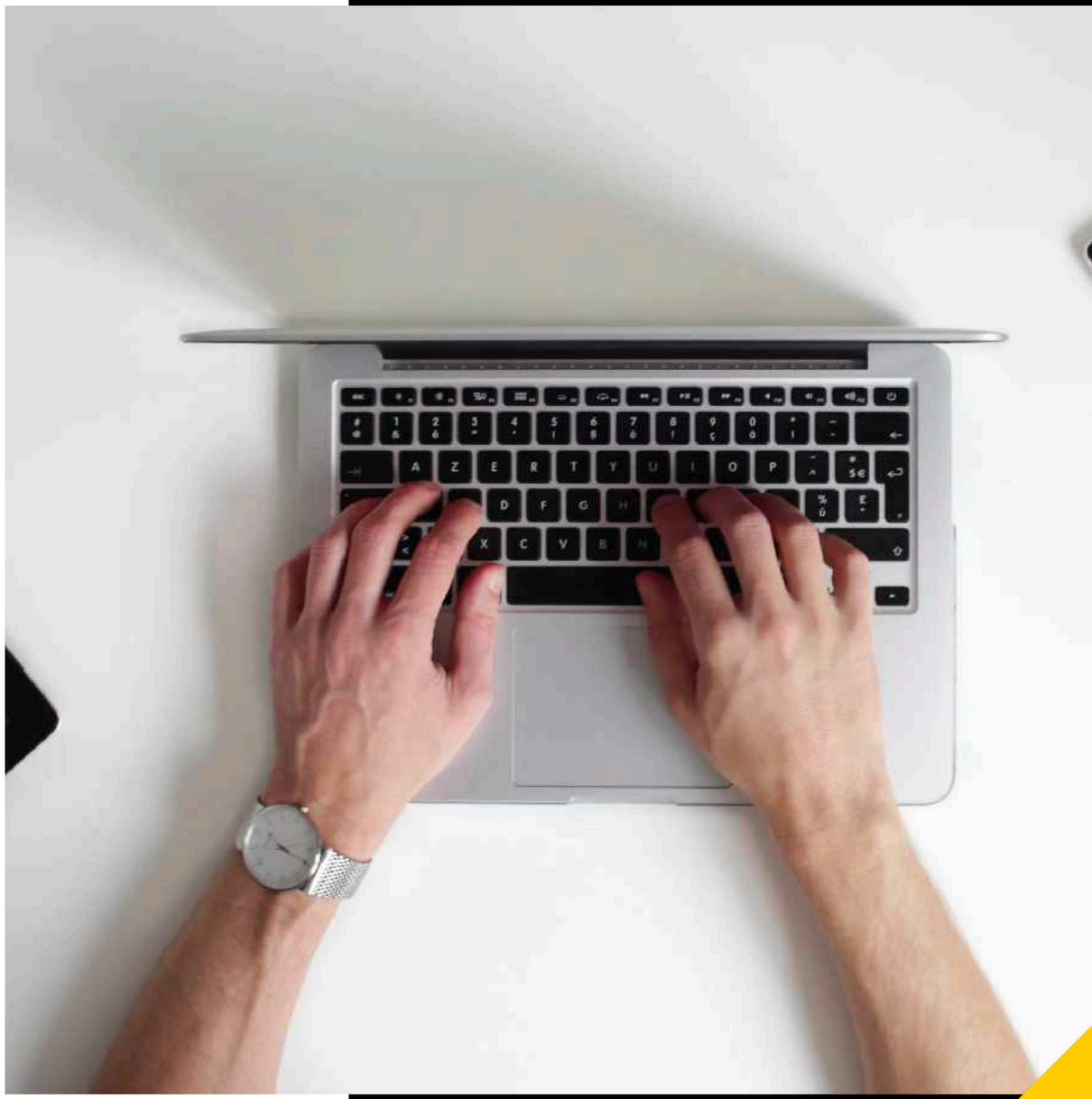
Meningkatkan kualitas confidentiality, integrity dan availability data atau informasi perusahaan

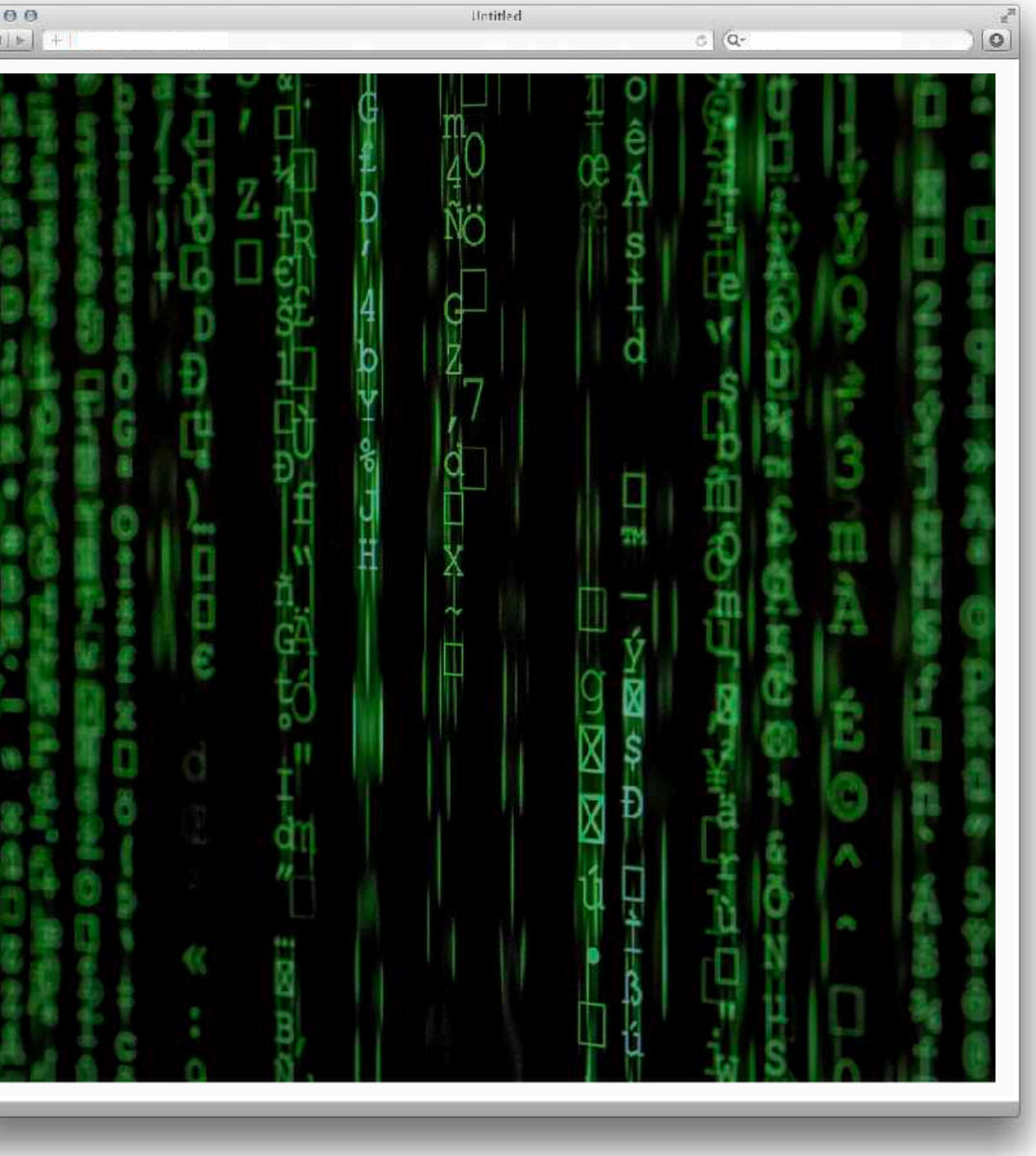
3. Melindungi usaha Anda

Pentest dapat mengurangi risiko terjadinya data breach yang dapat mempengaruhi reputasi bisnis Anda

Tipe Pengujian Penetrasi

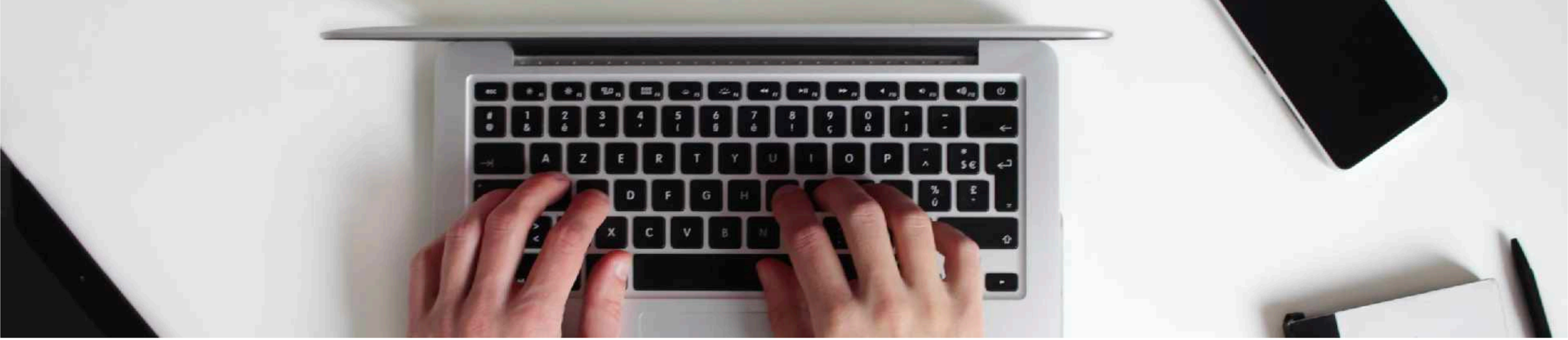
Banyaknya serangan siber yang terjadi tentunya akan meningkatkan ancaman siber pada suatu organisasi perusahaan, ancaman siber dapat mengganggu proses bisnis bahkan juga dapat mempengaruhi reputasi dari perusahaan tersbut. Untuk itu Penetration testing perlu dilakukan. Mengapa ???





1. Infrastruktur Jaringan

Pengujian dilakukan pada Infrastruktur dan jaringan operasional yang sedang berjalan baik *wireless* ataupun *wired* dan mencoba mengeksploitasi kerentanan yang ada, pada penetrasi test tipe ini akan dilakukan pengujian terhadap servis yang berjalan, pathing update, konfigurasi yang tidak aman, celah pada implentasi jaringan dan lain sebagainya



2. Aplikasi

Pengujian dilakukan terhadap aplikasi yang digunakan atau dikembangkan oleh perusahaan baik itu aplikasi mobile atau aplikasi web, pengujian pada tipe ini akan menitik beratkan pada bagaimana konsep security diterapkan oleh developer atau pemrogram pada aplikasi yang dikembangkan. Pengujian penetrasi pada aplikasi biasanya akan mengeksploitasi kerentanan seperti pada session/configuration manajemen, data proteksi, error handling, input proteksi dan lain-lain.

3. Sumber Daya Manusia (Social Engineering)

Pengujian tidak hanya dilakukan terhadap infrastruktur dan application system based saja, tapi dalam konsep security pengujian terhadap sumber daya manusia juga perlu dilakukan, hal ini dilakukan bertujuan untuk mengukur seberapa aware-nya sumber daya manusia dalam suatu organisasi dalam hal keamanan informasi. Hal ini penting karena manusia memegang peranan penting terhadap suatu kebijakan keamanan yang telah ditetapkan. Social engineering adalah metode yang dilakukan tipe pengujian ini dengan cara memanipulasi sisi psikologis dari manusia, banyak cara yang bisa dilakukan beberapa diantaranya adalah melalui phising, phone cells dan lainnya.

Summary.

Penetration testing adalah metodologi yang dilakukan sebagai bentuk kontrol terhadap upaya pencegahan dari risiko-risiko keamanan siber yang mungkin terjadi pada proses bisnis suatu perusahaan selain itu Penetration testing dapat berguna untuk meningkatkan kemanan informasi sehingga reputasi perusahaan dapat terjaga, dengan menggunajan hasil pengujian penetrasi perusahaan diharapkan dapat berbenah dan melaksanakan proses pengamanan informasi dengan lebih baik.

KONTAK KAMI

LOGIQUE DIGITAL INDONESIA

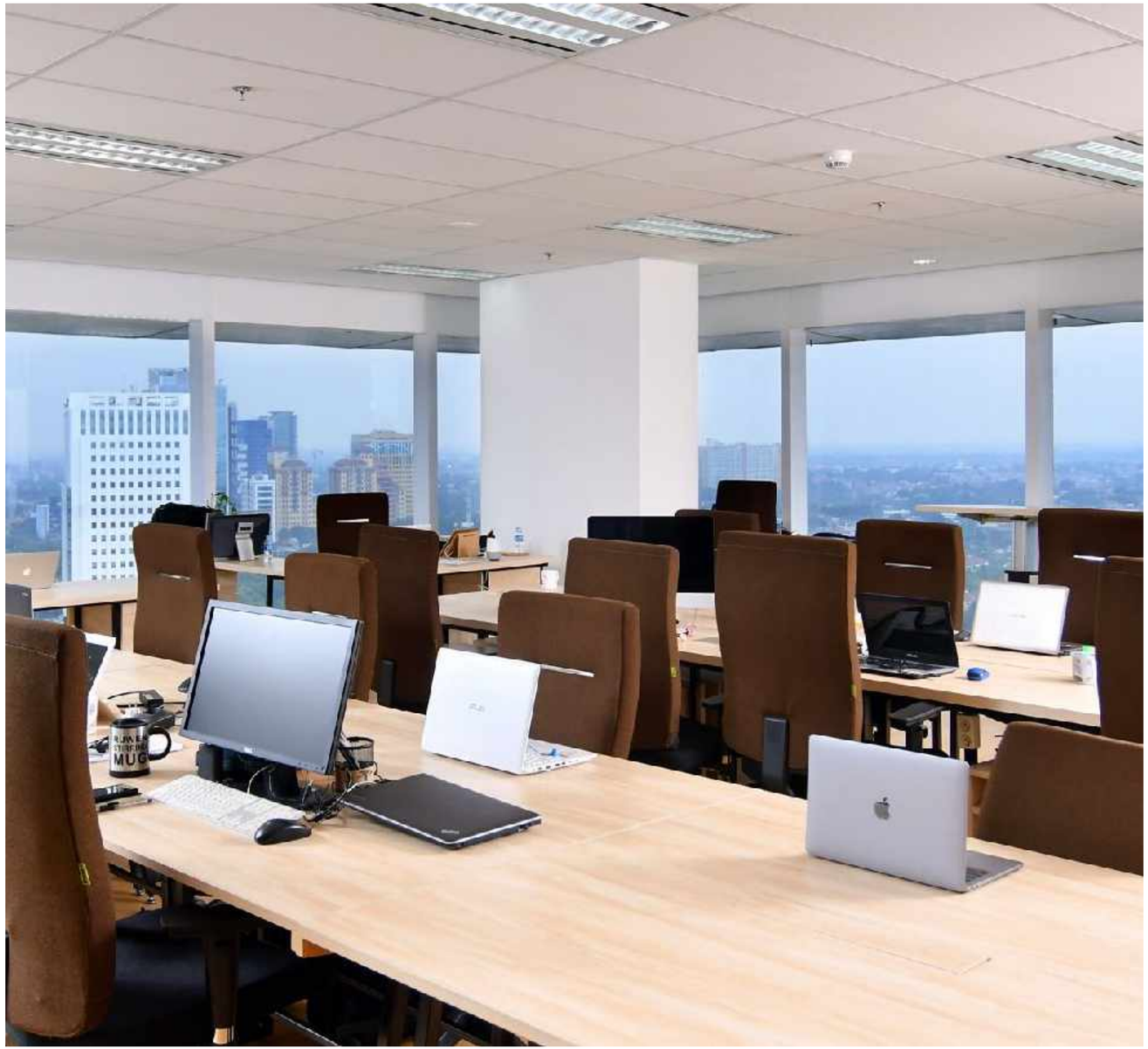
Ad Premier Building 19th Floor.
Jalan Tb. Simatupang No. 5
Ragunan, Ps. Minggu, Jakarta Selatan,
Indonesia 12550

info@logique.co.id

+62 21 22708935 / 36

+62 811 870 321

**nomor selular dan whatsapp*



logiquedigital