PERBANKAN DARING

KEWASPADAAN KEAMANAN

> Informasi berikut menawarkan sejumlah rekomendasi untuk meningkatkan kewaspadaan Anda dan melindungi aktivitas daring Anda. Anda disarankan untuk meninjau dokumen ini secara berkala agar tetap waspada terhadap ancaman keamanan yang terus berkembang.

Risiko Perbankan melalui Internet

Malware

Malware, singkatan dari *malicious software*, adalah perangkat lunak yang digunakan atau diprogram oleh penyerang untuk mengganggu operasi komputer, mengumpulkan informasi sensitif, atau mendapatkan akses ke sistem komputer pribadi.

Malware adalah istilah umum yang digunakan untuk merujuk pada berbagai bentuk perangkat lunak berbahaya atau intrusif, termasuk virus komputer, worm, Trojan horse, keylogger, spyware, dan program berbahaya lainnya.

Penipu dapat menggunakan teknik Phishing atau Social Engineering untuk memasang malware di komputer Anda.

Phishing

Phishing adalah bentuk rekayasa sosial dengan tujuan mendapatkan informasi rahasia yang sensitif secara curang. Surel phishing biasanya memiliki satu atau beberapa karakteristik berikut: tampak berasal dari pengirim yang sah; subjek surel menyampaikan pesan penting; isi surel mungkin menjanjikan manfaat bagi penerima, atau meminta balasan yang mendesak dan dapat menimbulkan konsekuensi jika tidak dipatuhi; dan mungkin meminta penerima untuk mengeklik tautan atau mengunduh lampiran. Surel tersebut dapat berisi tautan yang memicu serangan, atau tautan yang mengarahkan penerima ke situs web palsu atau lampiran berkas yang rusak.

Disarankan agar Anda berhati-hati dan hanya mengklik tautan ke situs web tepercaya, jangan membuka lampiran surel yang tampak mencurigakan, dan jangan memberikan informasi sensitif ke situs *web* yang tidak dikenal. Penipu sering kali memikat klien untuk menggunakan kredensial mereka.

(misalnya ID masuk, kata sandi, dan kata sandi sekali pakai (OTP) yang dihasilkan dari perangkat keamanan) di halaman *web* palsu.

Rekayasa Sosial

Rekayasa sosial adalah istilah yang menggambarkan jenis intrusi non-teknis yang sangat bergantung pada interaksi manusia dan sering kali melibatkan manipulasi perilaku manusia untuk melanggar langkah-langkah keamanan yang telah ditetapkan.

Biasanya, seorang penipu akan menyamar sebagai pihak lawan yang dapat dipercaya untuk mengekstrak informasi rahasia dari seorang karyawan yang akan memungkinkan akses ke infrastruktur organisasi, menggunakan skenario yang telah dikuasai dengan baik, seperti

Tipuan CEO Palsu:

Panggilan telepon dan/atau surel dari individu yang mengaku sebagai bagian dari Manajemen Senior perusahaan Anda, meminta transfer dana dalam jumlah besar yang mendesak dan rahasia untuk alasan yang sangat rahasia (misalnya pengambilalihan, alasan pajak, atau transaksi rahasia yang besar)

Tipuan Pemasok Palsu:

Panggilan telepon dan/atau surel dari seseorang yang menyamar sebagai pemasok Anda, memberitahukan perubahan rincian rekening bank, dan meminta untuk melakukan pembayaran di masa mendatang ke rekening penipuan

Tipuan Teknisi Palsu:

Panggilan telepon dari seseorang yang menyamar sebagai layanan bank Anda atau pemasok perangkat lunak Anda, dengan dalih migrasi, uji coba, peningkatan sistem perbankan elektronik Anda. Penipu umumnya meminta Anda untuk mengizinkannya mengakses perangkat Anda dari jarak jauh, yang memungkinkannya melakukan transfer palsu

BNP Paribas tidak akan pernah menghubungi Anda untuk meminta informasi akun Anda. Jika Anda dihubungi untuk memberikan informasi akun, jangan memberikannya.

Praktik Keamanan BNP Paribas

BNP Paribas berkomitmen penuh dalam melindungi aset informasi, data, dan informasi kliennya. BNP Paribas berupaya menangani data secara aman melalui pendekatan pertahanan berlapis, yang bertujuan untuk melindungi aset informasi BNP Paribas dan kliennya dari pengumpulan, penyimpanan, penggunaan, pengungkapan, modifikasi, atau penghancuran yang tidak sah. Pendekatan ini dilakukan melalui kebijakan, prosedur, pedoman, dan arsitektur keamanan teknis yang tepat.

Kebijakan dan pengendalian keamanan informasi BNP Paribas dievaluasi secara berkelanjutan untuk memastikan relevansi dan keselarasan dengan standar industri dan persyaratan peraturan. Kebijakan dan prosedur BNP Paribas mencakup area keamanan informasi penting, termasuk:

Pengendalian Akses

Akses ke sistem dan platform diberikan berdasarkan hak istimewa paling rendah dan seperlunya saja. Semua akses diberikan berdasarkan profil pengguna sesuai dalam platform Manajemen Hak Akses dan dengan persetujuan sebelumnya. Penggunaan media yang dapat dilepas, dikendalikan dan secara bawaan adalah dilarang.

Keamanan Aplikasi

Aplikasi tunduk pada proses sertifikasi keamanan sesuai dengan Kebijakan Keamanan Informasi BNP Paribas dan standar pengembangan aplikasi yang aman. Audit dan pengujian penetrasi rutin memvalidasi kekuatan aplikasi sensitif.

Pengendalian Perubahan

Implementasi perubahan sistem dan platform dikendalikan dengan menggunakan prosedur pengendalian perubahan formal. Perubahan memerlukan persetujuan manajemen sebelum diimplementasikan dalam lingkungan *production*.

Ketersediaan Data

Sistem dan data BNP Paribas dicadangkan secara aman untuk pemulihan jika diperlukan. Sistem cadangan atau pemulihan bencana yang diperlukan telah tersedia untuk memastikan ketahanan sistem dan data jika terjadi ketidaktersediaan lingkungan *production* yang tidak terduga.

Kerahasiaan Data

Protokol jaringan aman digunakan untuk lalu lintas sensitif, dan dilengkapi dengan solusi teknis untuk mendeteksi atau memblokir pengambilan data dari jaringan BNP Paribas. Enkripsi digunakan untuk transmisi data melalui jaringan publik dan pada perangkat media *portable*.

Pemulihan Bencana

BNP Paribas telah menerapkan kebijakan dan prosedur untuk melindungi manusia, fasilitas, infrastruktur, proses bisnis, aplikasi, dan data sebelum, selama, dan setelah peristiwa bencana. Respon dan pemulihan sistem aplikasi dan proses bisnis yang penting telah direncanakan dan diuji dengan cermat. Metodologi pemulihan bencana BNP Paribas mencakup hal-hal berikut:

- ✓ Analisis dampak bisnis
- ✓ Rencana pemulihan bencana aplikasi yang kritis
- ✓ Pengujian rutin rencana pemulihan bencana untuk memverifikasi kesiapan operasional

Tata Kelola

Tim keamanan khusus bekerja sama secara lokal, regional, dan global di dalam Grup BNP Paribas. Tim-tim tersebut disusun dalam posisi-posisi khusus yang memastikan cakupan keamanan aplikasi, sistem, dan data yang berkelanjutan, serta respons yang tepat terhadap insiden keamanan.

Seorang CISO (Chief Operating Security Officer) lokal mengawasi pengaturan, memelihara kerangka kerja kebijakan keamanan, dan berupaya memastikan strategi keamanan tepat untuk mencakup risiko keamanan yang berlaku pada lingkungan operasional dan regulasi.

Pengamanan Fisik

Langkah-langkah keamanan fisik telah diterapkan dan dirancang untuk menyediakan akses terbatas dan terekam, serta mendeteksi dan mencegah intrusi.

Langkah-langkah telah diterapkan untuk memberi tahu petugas keamanan fisik tentang kondisi lingkungan yang merugikan yang dapat memengaruhi sistem komunikasi elektronik.

Manajemen Pemasok

Program Manajemen Vendor BNP Paribas dilakukan secara uji tuntas terhadap aktivitas pihak ketiga, termasuk namun tidak terbatas pada keamanan informasi, pengadaan, dan privasi data, termasuk:

- ✓ Evaluasi calon vendor untuk kepatuhan terhadap kebijakan dan pengendalian BNP Paribas.
- ✓ Tinjauan uji tuntas, termasuk penyusunan peringkat risiko dan temuan.
- ✓ Mitigasi temuan risiko

SDM

Proses rekrutmen mencakup pemeriksaan keamanan individu sebelum penerimaan. Program kesadaran keamanan memastikan karyawan mengetahui risiko dan dapat bereaksi dengan tepat. Kebijakan keamanan BNP Paribas menegakkan tugas dan tanggung jawab karyawan terkait perlindungan data.

Perlindungan Jaringan

Kontrol akses jaringan diterapkan untuk memisahkan segmen jaringan BNP Paribas dan memantau lalu lintas masuk dan keluar dengan pihak eksternal, serta pemantauan dan deteksi intrusi 24/7.

Perlindungan Sistem

Perlindungan malware dipasang di semua titik kunci jaringan dan diperbarui secara berkala untuk memastikan deteksi dan penghapusan kode berbahaya secara cepat. Selain itu, dasar konfigurasi menegakkan penerapan system aman yang konsisten. Program *patching* memastikan perlindungan sistem BNP Paribas terkini, dengan fokus pada pembaruan keamanan. Pemeriksaan kerentanan berkala memastikan bahwa tidak ada sistem yang terlewatkan

Manajemen Kerentanan

Tim Manajemen Kerentanan Operasi Keamanan BNP Paribas bertanggung jawab atas manajemen kerentanan, dan melakukan pemindaian untuk menganalisis aset informasi. Kontrol mitigasi diterapkan jika diperlukan, dan program perbaikan diterapkan dengan memprioritaskan aset penting.

Tanggapan terhadap Ancaman

Tim respons insiden regional mengelola, mengendalikan, dan memulihkan insiden terkait keamanan serta memantau efektivitas kontrol tersebut. BNP Paribas memiliki layanan intelijen ancaman, yang memperbarui dan memperkaya konsol keamanannya melalui intelijen ancaman yang telah diverifikasi dan bersumber dari eksternal. Pertahanan BNP Paribas senantiasa waspada terhadap setiap ancaman siber yang diketahui.

Jika terjadi pelanggaran, tim respon insiden akan segera mengambil tindakan untuk mengamankan informasi, menyelidiki masalah tersebut, dan memitigasi pelanggaran. Notifikasi kepada klien yang terdampak disampaikan sebagaimana berlaku sesuai dengan persyaratan kontraktual, peraturan, dan perundang-undangan.

Intelijen Ancaman

BNP Paribas telah menetapkan proses untuk pengumpulan dan analisis ancaman di dunia maya, yang dirancang khusus untuk lanskap ancaman dan vertikal industri BNP Paribas.

Fungsi Intelijen Ancaman berupaya untuk tetap unggul dari pelaku dunia maya melalui intelijen yang tepat waktu, akurat, dan relevan.

Sertifikasi

Sebagai bagian dari komitmennya terhadap kualitas dan keamanan, BNP Paribas telah mengajukan sertifikasi untuk proses-proses utama yang terkait dengan eksploitasi dan pengembangan platform Connexis Cash:

Bersertifikat ISO:9001 – standar untuk manajemen kualitas, yang diberikan kepada eksploitasi dan infrastruktur platform Connexis Cash

Bersertifikat ISO:20000 – standar untuk manajemen layanan TI, yang diberikan kepada eksploitasi dan infrastruktur platform Connexis Cash

Bersertifikat ISO:27001 – standar untuk manajemen keamanan informasi, yang diberikan kepada eksploitasi dan infrastruktur platform Connexis Cash dan juga untuk pengembangan dan pengelolaan platform Connexis Cash itu sendiri

Rekomendasi

Untuk membantu menghindari tindakan penipuan dan pengungkapan data rahasia, BNP Paribas menyarankan Anda untuk memperhatikan 10 rekomendasi berikut terkait manajemen alur kerja dan perlindungan infrastruktur

1 Terapkan Prinsip 4-mata

Patuhi prinsip 4-mata untuk semua layanan utama seperti pengelolaan hak, otorisasi pembayaran, dan pengelolaan penerima manfaat.

2 Tinjau Akses Pengguna

Administrator TI harus meninjau akses pengguna setidaknya sekali per tahun

3 Selalu Gunakan Perangkat Lunak Terbaru

Perangkat lunak mencakup sistem operasi (misalnya Microsoft Windows), peramban (misalnya Internet Explorer, Firefox, Chrome), dan perangkat lunak penting lainnya (misalnya Java, Flash, Antivirus, Firewall dan Anti-Spyware). Perangkat lunak dan *patch* harus diperbaharui secara rutin.

4 Jaga Kerahasiaan Informasi Pribadi

Token dan kata sandi bersifat pribadi dan tidak boleh diungkapkan kepada siapa pun. Sangat penting untuk mengamankan kredensial login karena data ini memudahkan akses ke platform BNP Paribas. Panduan berikut dapat membantu menjaga keamanan informasi pribadi Anda:

- ✓ Jangan menduplikasi nama pengguna dan kata sandi yang sama dengan yang Anda gunakan untuk *login* situs *web* lain, baik pribadi maupun terkait pekerjaan;
- ✓ Jangan gunakan informasi yang mudah disalahpahami, seperti tanggal lahir atau nomor telepon;
- ✓ Meskipun ID pengguna Anda (biasanya alamat surel) tidak bersifat rahasia, jangan menuliskannya di tempat yang mudah ditemukan oleh orang yang tidak bertanggung jawab;
- ✓ Jangan pernah menuliskan atau mengungkapkan kata sandi digital, nomor seri SecurID, atau nomor PIN kepada siapa pun, termasuk Tim Dukungan BNP Paribas;
- ✓ Ubah kata sandi Anda secara berkala;
- ✓ Pastikan Anda tidak diawasi saat memasukkan kata sandi;
- ✓ Periksa *keyboard* dan komputer Anda secara berkala untuk memastikan tidak ada *keylogger* (perangkat yang merekam penekanan tombol) yang terhubung secara tidak sah;
- ✓ Banyak peramban memiliki fungsi pelengkapan otomatis. Meskipun hal ini menghemat waktu pengguna, hal ini juga memungkinkan orang yang tidak berwenang untuk masuk ke akun Anda jika komputer Anda tidak terkunci dan tidak dijaga. BNP Paribas menyarankan agar Anda menonaktifkan fungsi pelengkapan otomatis peramban web Anda.
- ✓ **Apa pun situasinya, jangan pernah memberikan PIN/kode rahasia Anda kepada siapa pun (termasuk tim dukungan BNP Paribas) dan pastikan tidak ada seorang pun kecuali Anda yang mengetahuinya.**

Perangkat Otentikasi

- ✓ Jika Anda menerima token autentikasi atau kata sandi sekali pakai yang dikirimkan ke perangkat seluler, harap pastikan perangkat tersebut selalu aman.
- ✓ Jangan berkomunikasi melalui telepon atau ke alamat surel yang tidak dikenal mengenai nomor seri yang tertera di balik token, meskipun mengaku dari tim dukungan, kecuali Anda telah menghubungi tim dukungan terkait sebelumnya untuk pengaturan ulang PIN atau masalah sinkronisasi kartu. Jika terjadi masalah, Anda dapat mengomunikasikan nomor seri tersebut ke Meja Layanan Klien BNP Paribas untuk ditindaklanjuti.
- ✓ Dalam hal apa pun, jangan menempelkan atau menulis apa pun pada token SecureID.
- ✓ Jika Anda kehilangan atau yakin telah kehilangan token Anda, harap hubungi Meja Layanan Klien BNP Paribas sesegera mungkin agar kami dapat menonaktifkan token Anda.

Informasi Pribadi Anda:

- ✓ Harap selalu beri tahu BNP Paribas rincian akurat mengenai informasi pribadi Anda.

5 Lindungi Stasiun Kerja Anda dari Peretasan dan *Malware*

Ada beberapa cara untuk melindungi komputer Anda dari peretas, virus, dan program jahat.

Perangkat lunak antivirus, perangkat lunak *anti-spyware*, dan *firewall* pribadi harus diinstal dan selalu aktif di komputer Anda. Definisi *patch* keamanan dan virus harus diinstal dan diperbarui secara rutin untuk memastikan *bug* dan celah keamanan telah ditutup.

Lakukan pemindaian Antivirus dan Anti-Spybot secara berkala. Jika program antivirus atau *antispyware* Anda mendeteksi berkas yang mencurigakan, segera hapus berkas tersebut dan tutup situs web yang telah mengunduh berkas tersebut. Jika komputer telah disusupi, segera ubah semua kata sandi Anda. Jangan melakukan transaksi BNP Paribas melalui komputer umum atau bersama.

6 Jangan Tinggalkan Stasiun Kerja Anda Tanpa Pengawasan

Jangan meninggalkan stasiun kerja tanpa pengawasan saat masuk dan selalu ingat untuk keluar setelah transaksi e-banking selesai.

Sangat disarankan agar aplikasi browser ditutup sepenuhnya setelah menggunakan platform BNP Paribas apapun

7 Kunjungi Hanya Situs Web Terpercaya

Kunjungi hanya situs web tepercaya dan jangan mengunduh berkas atau program apa pun dari situs web yang tidak dikenal atau mencurigakan. Selalu validasi sumbernya saat membuka berkas yang tidak dikenal, surel yang aneh atau program baru, dan jangan pernah mengeklik tautan yang mencurigakan

8 Waspada surel Penipuan dan Situs *Web* yang Mengaku sebagai BNP PARIBAS

Waspadalah terhadap surel dan situs web mencurigakan yang mencoba melakukan penipuan untuk mencuri informasi sensitif. BNP Paribas tidak akan pernah meminta informasi pribadi Anda melalui surel dan tidak akan mengirim surel dengan tautan tertanam ke situs web transaksional.

Selalu verifikasi bahwa pengirim surel tepercaya sebelum membuka lampiran apa pun, dan jangan menanggapi atau mengklik tautan apa pun yang terdapat dalam pesan surel yang tampaknya dikirim oleh BNP Paribas, yang meminta Anda memasukkan data pribadi, nomor rekening bank/kartu, atau kode *Internet Banking*.

Perlu diketahui juga bahwa di beberapa aplikasi surel seperti Microsoft Outlook, tautan teks mungkin ditampilkan, tetapi tautan tersebut justru dapat mengarahkan Anda ke situs *web* lain. Ini bisa jadi merupakan serangan siber yang dikenal sebagai *phishing*, dan telah dijelaskan di atas. Situs *web phishing* dirancang agar terlihat identik dengan situs *web* asli.

Selain itu, beberapa surel mungkin berisi berkas gambar yang tampak seperti teks. Mengarahkan kursor ke gambar dan mengkliknya dapat mengarahkan Anda ke situs *web phishing*. Pastikan panduan untuk memverifikasi situs *web* BNP Paribas (di bawah) diikuti.

Menavigasi ke situs *web* BNP Paribas harus selalu dilakukan melalui tautan yang dikenal. Harap baca bilah alamat/URL dengan seksama dan selalu pastikan bahwa *domain*-nya benar. Situs web BNP Paribas adalah situs yang aman, ditandai dengan alamat yang diawali dengan "https". Huruf 's' di akhir https berarti komunikasi antara peramban *web* dan situs *web* yang Anda gunakan dienkripsi. Otoritas Sertifikasi (seperti Verisign atau Geotrust) adalah penerbit sertifikat digital pihak ketiga tepercaya yang memverifikasi bahwa URL situs *web* tersebut adalah situs asli Perusahaan atau bisnis yang bersangkutan. Anda dapat mengklik gembok di sebelah URL untuk melihat rincian Otoritas Sertifikasi.

9 Jangan Bertindak Atas Panggilan Mencurigakan dari BNP PARIBAS

Jika ada yang menelepon Anda dan mengaku bekerja untuk atau atas nama BNP Paribas, lalu meminta Anda memberikan data pribadi dan/atau memulai/mengesahkan transaksi, jangan melakukan tindakan apa pun dan segera hubungi Layanan Klien BNP Paribas (CSD).

10 Jika ragu, hubungi BNP PARIBAS

Segera batalkan transaksi apa pun dan hubungi BNP Paribas jika terdapat keraguan, terutama jika prosedur penandatanganan berbeda dari prosedur standar yang telah ditetapkan. Anda disarankan untuk memeriksa apakah semua transaksi yang sedang berlangsung sah atau tidak. Silakan hubungi Layanan Klien BNP Paribas (CSD).

Jika Anda menginginkannya akses tidak sah atau memiliki pertanyaan yang belum terjawab terkait Keamanan Informasi, silakan segera hubungi *Relationship Manager* Anda atau Layanan Klien BNP Paribas (CSD).

Penafian

Isi dari dokumen ini bersifat umum dan bukan merupakan nasihat hukum, keuangan, pajak atau profesional. Meskipun informasi yang dimuat dalam dokumen ini telah diperoleh dari sumber-sumber yang diyakini PT Bank BNP Paribas Indonesia dapat diandalkan, tidak ada pernyataan atau jaminan apa pun, tegas maupun tersirat, yang dibuat dan tidak ada tanggung jawab apa pun yang diterima atau akan diterima oleh PT Bank BNP Paribas Indonesia mengenai atau dalam kaitannya dengan keakuratan, keandalan atau kelengkapan dari informasi tersebut. Semua dan setiap tanggung jawab dan kewajiban tersebut secara tegas dan sepenuhnya disangkal.

Pendapat-pendapat yang dinyatakan dalam dokumen ini mencerminkan penilaian PT Bank BNP Paribas Indonesia pada tanggal dokumen ini dan dapat tunduk pada perubahan tanpa pemberitahuan apabila PT Bank BNP Paribas Indonesia mengetahui informasi apa pun, yang bersifat khusus ataupun umum, yang mungkin memiliki dampak material terhadap pendapat-pendapat tersebut.

Baik PT Bank BNP Paribas Indonesia maupun setiap afiliasinya atau direktur, pejabat atau karyawan masing-masing tidak bertanggung jawab atas setiap kerugian atau kerusakan yang diderita atau dialami oleh pihak mana pun akibat mengandalkan atau menggunakan dokumen ini.

Tidak ada hal apa pun dalam dokumen ini yang akan ditafsirkan sebagai pemberian atau penyerahan hak apa pun melalui lisensi atau sehubungan dengan setiap paten, hak cipta, merek dagang atau logo Grup BNP Paribas (termasuk pengetahuan teknis dan rahasia dagang) atau hak kekayaan intelektual lainnya.

Dokumen ini tidak dapat diproduksi kembali (secara keseluruhan maupun sebagian) dan tidak dapat diringkas atau didistribusikan tanpa persetujuan tertulis sebelumnya dari PT Bank BNP Paribas Indonesia.

PT Bank BNP Paribas Indonesia diatur dan diawasi oleh Otoritas Jasa Keuangan sebagai bank umum. Informasi dalam dokumen ini tidak dimaksudkan untuk didistribusikan kepada, atau digunakan oleh, atau bukan merupakan penawaran apa pun kepada, setiap orang atau badan di yurisdiksi manapun apabila (a) pendistribusian atau penggunaan atau penawaran informasi tersebut akan bertentangan dengan hukum atau peraturan, atau (b) PT Bank BNP Paribas Indonesia akan menjadi tunduk pada persyaratan hukum atau peraturan yang berlaku.

Dengan menerima dokumen ini, Anda sepakat untuk terikat pada pembatasan-pembatasan tersebut di atas.

version control 0725-01