Questions 1

1. Apakah cybersecurity menjadi prioritas di Target? Jelaskan.
2. Bagaimana keamanan yang lemah berdampak pada pendapatan

penjualan dan kinerja yang bagus?

1. Menurut para ahli, bagaimana pelanggaran data dilakukan?
2. Selain pencurian data, apa lagi yang dirusak oleh insiden ini?
3. Apakah insiden cybersecurity ini dapat diduga? Apakah itu bisa dihindari?
4. Mengapa manajemen tidak memperlakukan cyberthreats sebagai

prioritas utama?

1. Cari berita terbaru tentang pelanggaran data ini. Apakah Target sudah

pulih dari itu? Jelaskan.

1. Dengan asumsi bahwa CEO dan CIO dipaksa untuk mengundurkan diri,

pesan apa yang dikirimkan ke manajemen senior di perusahaan AS?

Jawab:

1. Para manajer tidak lagi mempertanyakan apakah jaringan mereka akan diserang, tetapi berapa banyak kerusakan yang akan dilakukan, berapa lama penyelidikan akan dilakukan, dan berapa banyak biaya penyelidikan dan denda.
2. Berdampak dalam kerugian penipuan dan denda serta beberapa uang untuk investigasi, remediasi, pemantauan kredit, dan asuransi pencurian identitas untuk konsumen yang terpengaruh. reputasi yang rusak, hukuman keuangan, denda pemerintah federal dan negara bagian, kehilangan pangsa pasar, jatuhnya harga saham, dan reaksi balik konsumen.
3. Secara khusus, malware mengidentifikasi proses yang terkait dengan pembaca kartu kredit dan mencuri kartu pembayaran Melacak 1 dan Melacak 2 data dari memorinya. Ini adalah data yang disimpan di strip magnetik kartu pembayaran yang digunakan untuk mengkloning atau membuat kartu palsu.
4. Data pribadi dan keuangan dari hingga 70 juta pelanggan dicuri oleh peretas menggunakan malware. Perkiraan pelanggaran biaya dari $ 400 juta menjadi $ 450 juta.
5. bisa, Berbulan-bulan sebelum serangan, pemerintah federal dan perusahaan penelitian swasta juga memperingatkan perusahaan tentang munculnya jenis malware baru (kode komputer berbahaya) yang menargetkan terminal pembayaran.
6. Pada saat peringatan, Target memperbarui terminal pembayaran, yang membuat mereka lebih rentan terhadap serangan, sebagai persiapan untuk musim liburan.
7. Enam bulan setelah pelanggaran, masih belum jelas kapan Target akan pulih sepenuhnya. Seorang analis keamanan di perusahaan teknologi Gartner memperkirakan biaya pelanggaran berkisar antara $ 400 juta hingga $ 450 juta. Itu termasuk tagihan yang terkait dengan denda dari perusahaan kartu kredit dan layanan untuk pelanggannya seperti pemantauan laporan kartu kredit gratis. Target juga menghadapi setidaknya 70 tuntutan hukum terkait dengan invasi privasi dan kelalaian, menuduh Target tidak mengambil langkah yang tepat untuk melindungi data konsumen.
8. "Ketika kami berencana untuk tahun fiskal baru, kami akan terus bekerja tanpa lelah untuk memenangkan kembali kepercayaan para tamu kami. . . . Kami didorong bahwa tren penjualan telah meningkat dalam beberapa minggu terakhir "

Questions 2

1. Mengapa menurut Anda smartphone yang dikeluarkan pemerintah adalah target pencurian data dan pencurian transmisi?
2. Tindakan pencegahan keamanan apa yang dilakukan Boeing sehubungan dengan pembuatan dan penjualan Black?
3. Fitur keamanan apa yang dibangun ke Black?
4. Mengapa enkripsi suara merupakan ukuran keamanan digital yang penting?
5. Mengapa model pertahanan mendalam penting untuk sebuah smartphone keamanan seperti Black?

Jawab

1. Smartphone dibuat pemerintah dibuat dengan maksud tertentu, berbeda dengan smartphone yang dibuat perusahaan untuk dipasarkan smartphone yang dibuat pemerintah dibuat untuk dibagikan karyawan pemerintah atau instansi pemerintah maka cracker selalu mencari cara agar dapat mencuri informasi dari pemerintah.
2. Telepon mengenkripsi komunikasi suara dan data dan, jika dirusak, merusak dirinya sendiri. Misalnya, setiap upaya membuka casing Black akan menghapus semua data dan perangkat lunak di perangkat dan membuatnya tidak dapat dioperasikan.
3. - Enkripsi untuk menyimpan informasi sensitif secara aman

- Roots of Trust (RoT) seperangkat fungsi dalam modul komputasi tepercaya untuk memastikan keaslian perangkat lunak

- Mesin kripto perangkat keras untuk melindungi data yang disimpan dan dikirim

- Komponen aman tertanam untuk mengaktifkan operasi tepercaya

- Modul platform tepercaya untuk menyediakan penyimpanan kunci yang aman

- Secure Boot untuk menjaga integritas gambar perangkat

1. untuk perusahaan yang bertujuan untuk menjaga data mereka dari taktik pengintaian NSA atau organisasi mata-mata lainnya. Black memungkinkan akses aman dan pertukaran data dan komunikasi penting pada perangkat seluler tepercaya.
2. Menurut pengajuan Boeing dengan Komisi Komunikasi Federal AS (FCC), Black dirancang untuk digunakan oleh lembaga pemerintah dan kontraktor yang perlu