Jurnal Ilmiah Wahana Pendidikan, Juni 2023, 9(12), 166-175
DOI: https://doi.org/10.5281/zenodo.8078569
p-ISSN: 2622-8327 e-ISSN: 2089-5364
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/JIWP

.

Manajemen Sekuriti pada Perusahaan Samsung Electronics Indonesia

Edy Susanto[1], Husni Fauzi Ramadhan[2] , Ivan Ardiansyah[3], Rizky Maulan[4]

[1] Fakultas Teknik, Universitas Bhayangkara Jakarta Raya
[2,3,4] Fakultas Ekonomi dan Bisnis, Universitas Bhayangkara Jakarta Raya

Received: 17 April 2023
Revised: 22 April 2023
Accepted: 22 Mei 2023

Abstract

During this time, the basic need for security has been established since the founding of the company. However, security measures are carried out only as they are, not consciously through more mature planning. In its activities, security management ensures that information resources remain secure and alert to their integrity, confidentiality, and availability so that they can minimize losses when unwanted things happen. Security management is to ensure that assets (buildings, machines), human resources (employees, visitors), and information systems (data, application programs) remain secure. The task and function of security management are to organize the safety and order in the environment or work area to prevent any disturbance of order and order or other violations of the rules of the company. Securities management is a part of overall management that covers the organizational structure, planning, responsibilities, implementation, procedures, processes, and resources necessary for the development, application, achievement, assessment, and maintenance of security policies in order to control the risks associated with business activities. Security management is based on the processing of data that is then analyzed about an event that has already occurred or may occur in a locality or environment. Security management is not only expected to keep information resources secure but also to keep the company functioning after a disaster or collapse of the security system.

Keywords: *Security Management*

(*) Corresponding Author: *edysusanto@gmail.com*

How to Cite: Susanto E, Ramadhan Husni F., Ardiansyah I, & Maulan R. (2023). Manajemen Sekuriti pada Perusahaan Samsung Electronics Indonesia. https://doi.org/10.5281/zenodo.8078569

PENDAHULUAN

Setiap perusahaan harus menentukan sendiri tingkat program sekuriti efektif yang dikehendakinya dan program itu sendiri harus ekonomis. Perusahaan juga harus menentukan langkah-langkah yang sesuai dengan kegunaannya.

Manajemen sekuriti yaitu suatu sistem untuk memberikan pemahaman yang utuh/ terpadu serta kemampuan dan keterampilan dalam merencanakan dan mendesain sistem pengamanan yang tepat, efektif, dan efisien, sesuai dengan situasi dan kondisi yang dihadapi, khususnya Ancaman / Gangguan yang mungkin terjadi serta untuk mencegah sedini mungkin kerugian-kerugian bagi Perusahaan (Loss Prevention).

Selama ini, kebutuhan dasar akan adanya sekuriti telah ditetapkan sejak berdirinya perusahaan. Namun, langkah-langkah sekuriti hanya dilakukan seadanya, tidak secara sadar melalui perencanaan yang lebih matang. Penerapan akan adanya sekuriti yang ditunjang oleh sistem-sistem yang menjalankannya dengan baik mejamin perusahaan untuk lebih tenang.

Manajemen sekuriti merupakan bagian dari manajemen secara keseluruhan yang meliputi struktur organisasi, perencanaan, tanggung jawab, pelaksanaan, prosedur, proses, dan sumber daya yang dibutuhkan bagi pengembangan penerapan, pencapaian, pengkajian dan pemeliharaan kebijakan

pengamanan dalam rangka pengendalian risiko yang berkaitan dengan kegiatan usaha guna mewujudkan lingkungan yang aman, efisien, dan produktif. Adapun adanya manajemen sekuriti (keamanan) ialah menjamin agar asset (gedung, perangkat mesin) sumber daya manusia (karyawan, visitor), dan system informasi (data, program aplikasi) agar tetap aman.

Tugas dan fungsi manajemen sekuriti adalah menyelenggarakan keamanan dan ketertiban di lingkungan atau Kawasan kerja dari setiap gangguan kemanan dan ketertiban serta pelanggaran lainnya yang menyangkut peraturan kerja perusahaan baik keamanan fisik personel maupun informasi.

Dalam aktivitasnya, manajemen sekuriti menjaga agar sumber daya informasi tetap aman dan terjaga integritas, kerahasiaan, dan ketersediaannya sehingga dapat meminimalisirkan kerugian apabila terjadi hal-hal yang tidak diinginkan. Manajemen sekuriti tidak hanya diharapkan untuk menjaga sumber daya informasi aman, namun juga diharapkan untuk menjaga perusahaan tersebut agar tetap berfungsi setelah suatu bencana atau jebolnya sistem keamanan.

Keberhasilan sekuriti efektif adalah pada sistem pencegahan yang menggunakan personel yang terampil dan terlatih dengan sebaik-baiknya, perlengkapan/peralatan modern yang efektif, dan perlengkapan elektronik yang akan menunjang pelaksanaan tugas sekuriti.

Dapat dikatakan juga sebagai kegiatan pengamanan yang terwujud dalam sistem atau tata cara kerja yang dilaksanakan secara teratur dalam aturan-aturan pelaksanaan tugas dalam suatu kawasan yang kesemuanya itu merupakan implementasi hubungan antara konsep manajemen dengan konsep sekuriti.

METODE

Samsung Electronics Co., Ltd. adalah perusahaan pembuat perangkat elektronika terbesar di dunia, dan berkantor pusat di Seocho Samsung Town di Seoul, Korea Selatan. Samsung Electronics dibentuk pada 1969 di Daegu, Korea Selatan dengan nama Samsung Electric Industries yang pada mulanya memproduksi perangkat elektronik seperti TV, kalkulator, kulkas, pendingin ruangan dan mesin cuci. Pada 1981, perusahaan ini telah memproduksi lebih dari 10 juta TV hitam-putih. Pada 1988, perusahaan ini bergabung dengan Samsung Semiconductor & Communications. Perusahaan ini adalah perusahaan Korea Selatan yang terbesar dan merupakan ikon dari Samsung Group, yang merupakan konglomerasi terbesar di Korea Selatan.

Samsung merupakan produsen besar komponen elektronik, seperti baterai ion litium, semikonduktor, sensor citra, modul kamera, dan layar untuk klien seperti Apple, Sony, HTC, dan Nokia. Perusahaan ini adalah produsen telepon seluler dan ponsel cerdas terbesar di dunia. Diawali dengan jajaran produk Samsung Solstice, yang kemudian dilanjutkan dengan Samsung Galaxy Perusahaan ini juga merupakan pemasok besar komputer tablet, terutama melalui jajaran produk Samsung Galaxy Tab yang dilengkapi dengan Android, serta dianggap mengembangkan pasar phablet, melalui Seri Samsung Galaxy Note. Perusahaan ini juga mengembangkan ponsel cerdas yang mendukung 5G, seperti Galaxy S21 dan Galaxy Note 20, serta ponsel lipat seperti Galaxy Z Flip 3 dan Galaxy Z Fold 3. Samsung pun merupakan produsen televisi terbesar di dunia sejak tahun 2006, dan merupakan produsen ponsel terbesar di dunia sejak tahun 2011. Perusahaan ini juga merupakan produsen chip memori terbesar di

dunia dan mulai tahun 2017 hingga 2018, sempat menjadi produsen semikonduktor terbesar di dunia, mengalahkan Intel.

Data dan privasi menjadi hal yang sangat penting di masa sekarang. Samsung pun mengembangkan sebuah ekosistem proteksi yang diberi nama dengan istilah Samsung Knox. Samsung menawarkan keamanan komprehensif dengan platform keamanan bersertifikat. Platform keamanan Knox Samsung adalah landasan perlindungan dalam perangkat pribadi,solusi bisnis perusahaan, dan layanan. Platform keamanan Knox terdiri atas berbagai lapisan mekanisme pertahanan dan keamanan yang melindungi data dari perangkat lunak dan ancaman berbahaya. Platform keamanan Knox telah terbukti dan di sertifikasi oleh berbagai lembaga pemerintah, badan sertifikasi keamanan, dan vendor keamanan pihak ketiga, sejak pelanggan mengaktifkan perangkat, platform Knox melindungi perangkat dan layanan.

Pemrogram Samsung telah membuat semacam add-on untuk sistem operasi, yang memungkinkan Anda untuk memberikan perlindungan maksimal kepada data pribadi pengguna. Program ini digabungkan sendiri beberapa ekstensi dibuat, dan menerima nama KNOX.

Ekstensi yang tersedia dirancang untuk menciptakan lingkungan yang aman bagi pengguna dengan mengisolasi zona tertentu, dan juga membuat booting menjadi sangat aman. Selain itu, program KNOX menggunakan metode enkripsi data khusus, sehingga meningkatkan tingkat keamanannya.

Selama pengoperasian normal aplikasi ini, pengguna dapat sepenuhnya yakin bahwa perangkat selulernya tidak terinfeksi spyware, dan juga terlindungi dengan baik dari peretasan jaringan.

KNOX, antara lain, memberi pengguna kemampuan untuk mengontrol aplikasi untuk akses ke sumber daya jaringan. Ini diimplementasikan melalui penggunaan yang dilindungi. Menggunakan perusahaan komunikasi mobile, melindungi data rahasia dari pencurian, karena perlindungan dibangun di semua arah utama - peretasan jaringan, implementasi ke dalam perangkat spyware, serta pembuatan semacam "bookmark" dengan memodifikasi kernel sistem. Bahkan jika ponsel Anda dicuri, penyerang tidak akan dapat menyalin informasi pribadi Anda.

Hal yang sama dapat dilakukan dengan aplikasi lain dan masuk ke dalamnya dengan login yang berbeda. Untuk mengakses program yang dilindungi, Anda harus memasukkan kata sandi atau gunakan.

Perlu dicatat fakta bahwa gagasan Samsung dapat memantau keadaan kernel sistem operasi dan integritasnya, dan kehadiran Time API memungkinkan Anda untuk mendapatkan informasi yang akurat tentang tanggal, waktu, dan zona waktu.

Sasarannya memang untuk menciptakan ekosistem seluler yang lebih baik dalam sebuah perusahaan. Meski demikian, kita tetap dapat memanfaatkannya untuk kepentingan pribadi karena Samsung Knox tertanam secara mendasar di dalam handphone buatan Samsung. Berbeda dari sistem proteksi pada umumnya (khususnya antivirus), Samsung Knox tidak akan berusaha untuk memblokir peranti lunak jahat melainkan memastikan bahwa data tidak disusupi meskipun mereka sudah masuk ke dalam perangkat.

Teknologi keamanan Knox yang tertanam kuat dalam produk Samsung sebagai berikut:

- Seluler
  Knox melindungi data rahasia dan sensitif secaraaman di setiap lapisan Perangkat Samsung Galaxy sejak perangkat dinyalakan, Knox senantiasa memberikan perlindungan waktu nyata.
- TV
  Knox secara aman menyediakan perlindungan lintas sektor terhadap data dan layanan pengguna dari perangkat Smart-TV Samsung hingga platform dan layanan online. Samsung menyediakan pengalaman TV yang aman dan optimal bagi pengguna.
- Peralatan Rumah Tangga
  Autentikasi Knox yang tangguh dan teknologi Kriptografi yang sudah terbukti, adalah tulang punggung untuk mengendalikan dan memantau secara aman peralatan rumah pintar Samsung yang didukung SmartThings dengan aman.

HASIL DAN PEMBAHASAN

Samsung Electronics Co., Ltd. adalah perusahaan pembuat perangkat elektronika terbesar di dunia, dan berkantor pusat di Seocho Samsung Town di Seoul, Korea Selatan. Samsung Electronics dibentuk pada 1969 di Daegu, Korea Selatan dengan nama Samsung Electric Industries yang pada mulanya memproduksi perangkat elektronik seperti TV, kalkulator, kulkas, pendingin ruangan dan mesin cuci. Pada 1981, perusahaan ini telah memproduksi lebih dari 10 juta TV hitam-putih. Pada 1988, perusahaan ini bergabung dengan Samsung Semiconductor & Communications. Perusahaan ini adalah perusahaan Korea Selatan yang terbesar dan merupakan ikon dari Samsung Group, yang merupakan konglomerasi terbesar di Korea Selatan.

Samsung merupakan produsen besar komponen elektronik, seperti baterai ion litium, semikonduktor, sensor citra, modul kamera, dan layar untuk klien seperti Apple, Sony, HTC, dan Nokia. Perusahaan ini adalah produsen telepon seluler dan ponsel cerdas terbesar di dunia. Diawali dengan jajaran produk Samsung Solstice, yang kemudian dilanjutkan dengan Samsung Galaxy Perusahaan ini juga merupakan pemasok besar komputer tablet, terutama melalui jajaran produk Samsung Galaxy Tab yang dilengkapi dengan Android, serta dianggap mengembangkan pasar phablet, melalui Seri Samsung Galaxy Note. Perusahaan ini juga mengembangkan ponsel cerdas yang mendukung 5G, seperti Galaxy S21 dan Galaxy Note 20, serta ponsel lipat seperti Galaxy Z Flip 3 dan Galaxy Z Fold 3. Samsung pun merupakan produsen televisi terbesar di dunia sejak tahun 2006, dan merupakan produsen ponsel terbesar di dunia sejak tahun 2011. Perusahaan ini juga merupakan produsen chip memori terbesar di dunia dan mulai tahun 2017 hingga 2018, sempat menjadi produsen semikonduktor terbesar di dunia, mengalahkan Intel.

Data dan privasi menjadi hal yang sangat penting di masa sekarang. Samsung pun mengembangkan sebuah ekosistem proteksi yang diberi nama dengan istilah Samsung Knox. Samsung menawarkan keamanan komprehensif

dengan platform keamanan bersertifikat. Platform keamanan Knox Samsung adalah landasan perlindungan dalam perangkat pribadi,solusi bisnis perusahaan, dan layanan. Platform keamanan Knox terdiri atas berbagai lapisan mekanisme pertahanan dan keamanan yang melindungi data dari perangkat lunak dan ancaman berbahaya. Platform keamanan Knox telah terbukti dan di sertifikasi oleh berbagai lembaga pemerintah, badan sertifikasi keamanan, dan vendor keamanan pihak ketiga, sejak pelanggan mengaktifkan perangkat, platform Knox melindungi perangkat dan layanan.

Pemrogram Samsung telah membuat semacam add-on untuk sistem operasi, yang memungkinkan Anda untuk memberikan perlindungan maksimal kepada data pribadi pengguna. Program ini digabungkan sendiri beberapa ekstensi dibuat, dan menerima nama KNOX.

Ekstensi yang tersedia dirancang untuk menciptakan lingkungan yang aman bagi pengguna dengan mengisolasi zona tertentu, dan juga membuat booting menjadi sangat aman. Selain itu, program KNOX menggunakan metode enkripsi data khusus, sehingga meningkatkan tingkat keamanannya.

Selama pengoperasian normal aplikasi ini, pengguna dapat sepenuhnya yakin bahwa perangkat selulernya tidak terinfeksi spyware, dan juga terlindungi dengan baik dari peretasan jaringan.

KNOX, antara lain, memberi pengguna kemampuan untuk mengontrol aplikasi untuk akses ke sumber daya jaringan. Ini diimplementasikan melalui penggunaan yang dilindungi. Menggunakan perusahaan komunikasi mobile, melindungi data rahasia dari pencurian, karena perlindungan dibangun di semua arah utama - peretasan jaringan, implementasi ke dalam perangkat spyware, serta pembuatan semacam "bookmark" dengan memodifikasi kernel sistem. Bahkan jika ponsel Anda dicuri, penyerang tidak akan dapat menyalin informasi pribadi Anda.

Hal yang sama dapat dilakukan dengan aplikasi lain dan masuk ke dalamnya dengan login yang berbeda. Untuk mengakses program yang dilindungi, Anda harus memasukkan kata sandi atau gunakan. Perlu dicatat fakta bahwa gagasan Samsung dapat memantau keadaan kernel sistem operasi dan integritasnya, dan kehadiran Time API memungkinkan Anda untuk mendapatkan informasi yang akurat tentang tanggal, waktu, dan zona waktu.

Sasarannya memang untuk menciptakan ekosistem seluler yang lebih baik dalam sebuah perusahaan. Meski demikian, kita tetap dapat memanfaatkannya untuk kepentingan pribadi karena Samsung Knox tertanam secara mendasar di dalam handphone buatan Samsung. Berbeda dari sistem proteksi pada umumnya (khususnya antivirus), Samsung Knox tidak akan berusaha untuk memblokir peranti lunak jahat melainkan memastikan bahwa data tidak disusupi meskipun mereka sudah masuk ke dalam perangkat.

Teknologi keamanan Knox yang tertanam kuat dalam produk Samsung sebagai berikut:

- Seluler

  Knox melindungi data rahasia dan sensitif secaraaman di setiap lapisan Perangkat Samsung Galaxy sejak perangkat dinyalakan, Knox senantiasa memberikan perlindungan waktu nyata.
- TV

Knox secara aman menyediakan perlindungan lintas sektor terhadap data dan layanan pengguna dari perangkat Smart-TV Samsung hingga platform dan layanan online. Samsung menyediakan pengalaman TV yang aman dan optimal bagi pengguna.

- Peralatan Rumah Tangga
  Autentikasi Knox yang tangguh dan teknologi Kriptografi yang sudah terbukti, adalah tulang punggung untuk mengendalikan dan memantau secara aman peralatan rumah pintar Samsung yang didukung SmartThings dengan aman.

PT Samsung Electronics Indonesia menggandeng perusahaan penyedia sistem integrator Malifax dalam meluncurkan sistem keamanan terintegrasi untuk piranti *gadget* bagi *enterprise*, yang diberi nama KNOX. Sistem yang berjalan di platform Android ini ditunjang oleh Malifax Corporate Mobility Solution (MCMS). Solusi ini bertujuan mengendalikan serta memisahkan data perusahaan dan pribadi yang ada di perangkat. Sehingga, data perusahaan dan pribadi tidak akan bercampur meski sama-sama tersimpan di satu perangkat. Dua hal yang diusung oleh KNOX yaitu pengaturan perangkat bergerak yang digunakan oleh pegawai serta jaminan keamanan data. "Platform ini dirancang untuk memudahkan kolaborasi di perangka."

Sejumlah keunggulan KNOX. Pertama, pengaturan fungsi keamanan dan aplikasi, di antaranya surat elektronik, daftar kontak, dan kalender. KNOX memisahkan informasi perusahaan dan pribadi ke dalam peyimpanan yang disebut *container*. Perangkat bergerak yang sudah ter-*install* aplikasi KNOX akan memunculkan lambang kunci di laman utama. Ketika diklik, secara otomatis akan muncul *container* yang berisi informasi perusahaan. Kedua, kemampuan enkripsi di setiap data. Jika perangkat bergerak dicuri atau hilang, perintah menghapus data dapat dilakukan. "Data yang dihapus dapat dikembalikan dengan cara mengenkripsinya". Ketiga adalah kemudahan pengaturan manajemen perusahaan. Sistem tersebut dapat digunakan untuk mengeluarkan peraturan, misalnya larangan untuk *browsing* atau penggunaan kamera saat sedang di kantor. Bahkan pengaturan juga terhubung ke toko *online* Google Play.

1. Risk Assasments Manajemen Sekuriti

Skenario 1 serangan siber : Akses backdoor tanpa persetujuan

Di luar Samsung, pengembang secara rutin membuat backdoor atau 'pintu rahasia' untuk aplikasi dan bahkan sistem operasi (OS) seluler sehingga mereka dapat memperoleh akses yang mudah saat perlu melakukan troubleshooting. Namun, peretas dapat menemukan backdoor ini, yang biasanya melompati satu atau semua pengaman siber pada perangkat yang dimaksud.

Untuk mencegah akses backdoor tanpa persetujuan, jangan mengunduh aplikasi tidak resmi atau tidak sah. Mengunduh perangkat lunak selain yang dipasang pabrikan sejak awal untuk mendapatkan akses penuh ke sistem operasi perangkat juga dapat mengundang malware atau spyware yang mengarah ke akses backdoor tanpa persetujuan.

Di Samsung, kami merancang, membuat, dan memvalidasi setiap chip komputer, setiap kabel, dan setiap komponen perangkat keras sebelum menggunakannya untuk memproduksi perangkat pintar kami di pabrik yang sangat aman di seluruh dunia. Pendekatan ini memberi kami kendali atas desain,

manufaktur, dan perakitan, memastikan rantai pasokan aman yang mencegah akses backdoor tanpa persetujuan di perangkat kami – menghasilkan produk yang dapat dipercaya sepenuhnya oleh konsumen.

Skenario 2 serangan cyber : password yang bocor, lemah, atau dipakai ulang

Seiring perkembangan jaman, kita terus membuat akun baru untuk berbagai layanan digital, mulai dari layanan konsultasi dokter online, platform transportasi online hingga e-commerce baru. Tanpa disadari hal ini menyediakan lebih banyak jalan untuk dieksploitasi oleh peretas.

Seperti yang ditemukan oleh IBM di survei Agustus 2021, 86% konsumen di Asia Pasifik mengakui bahwa mereka menggunakan kembali password yang sama di beberapa akun online. Hal ini merupakan sebuah kebiasaan privasi data yang buruk – dimana satu serangan saja dapat membuat seluruh jejak internet pengguna rentan disalahgunakan peretas.

Perangkat Samsung dilengkapi dengan teknologi otentikasi biometrik yang inovatif, seperti Ultrasonic Fingerprint, sehingga akses ke data Anda dapat dilindungi meskipun perangkat Anda hilang atau dicuri. Dikenal sebagai Samsung Pass, alat otentikasi biometrik ini juga memungkinkan pengguna dengan mudah mengakses kredensial masuk tanpa perlu mengingat nama pengguna dan kata sandi yang tak terhitung jumlahnya.

Untuk meningkatkan perlindungan data, Samsung juga telah melengkapi perangkat dengan Knox Vault, prosesor aman yang beroperasi secara independen dari CPU utama. Knox Vault mengisolasi data biometrik Anda dengan aman dari bagian lain ponsel Anda, sehingga tidak ada yang bisa mendapatkan data Anda.

Skenario 3 serangan siber : Wi-Fi gratis yang ternyata tidak sepenuhnya gratis

Hotspot Wi-Fi gratis adalah anugerah bagi semua orang yang membutuhkan akses Internet di perangkat seluler mereka untuk bekerja atau bermain. Namun, layanan Wi-Fi publik memberikan peluang bagi peretas untuk mencuri data, karena data yang Anda kirim melalui web – seperti informasi kartu kredit saat melakukan pembelian online – mungkin jatuh ke tangan peretas melalui jaringan Wi-Fi publik.

Untuk browsing sehari-hari, Secure Wi-Fi di perangkat Samsung mengenkripsi lalu lintas internet keluar dan menonaktifkan pelacakan pada aplikasi dan situs web. Hal ini memungkinkan Anda untuk menjelajah internet dengan aman pada Wi-Fi publik tanpa takut akan pelanggaran keamanan.

Skenario 4 Serangan Siber: Serangan phishing yang mengambil data sensitive

Phishing adalah jenis serangan di mana penjahat siber mengelabui korbannya untuk menyerahkan informasi sensitif atau memasang malware, menyamar sebagai tautan, lampiran, atau bahkan aplikasi yang sah, di perangkat mereka.

Setelah peretas memiliki akses ke informasi sensitif Anda, mereka dapat menggunakannya untuk meminta tebusan dari Anda, mencuri informasi pribadi Anda, melakukan kejahatan lain, bahkan melakukan pembelian dengan informasi kartu kredit Anda.

Samsung melindungi Anda dari ancaman ini lewat Device Protection di Samsung Device Care yang terus-menerus memindai perangkat Anda dari

malware atau aktivitas mencurigakan dan memperingatkan Anda saat Anda salahcmemasang aplikasi berbahaya melalui deteksi melalui perlindungan McAfee.

Selain itu, Samsung Secure Folder menjaga keamanan data dan mengisolasi aplikasi bermasalah di dalam folder untuk menjauhkan aplikasi dari informasi pribadi pengguna.

Skenario 5 Serangan Siber: Kerentanan zero-day

Mengingat peretas dan penyerang siber terus-menerus mencoba meretas perangkat, mereka selalu waspada terhadap kerentanan zero-day. Kerentanan zero-day adalah kerentanan dalam sistem atau perangkat yang telah ditemukan tetapi belum ditambal. Ini bisa sangat berbahaya karena penjahat dunia maya menargetkan kelemahan dalam sistem sebelum pengembang atau publik menyadarinya.

Samsung Knox menawarkan perlindungan secara real time, selalu secara aktif melindungi perangkat Anda dari serangan data atau malware. Ini berarti bahwa upaya tidak sah untuk mengakses atau memodifikasi ponsel Anda diblokir secara real time.

Saat pengguna melakukan reboot pada smartphone Samsung mereka, Secure Boot diaktifkan untuk mendeteksi perangkat lunak yang tidak sah dan memblokir upaya untuk menyusupi perangkat melalui keamanan berlapis tingkat militer. Jika smartphone di-boot dalam keadaan tidak disetujui, Samsung Knox akan secara otomatis mengunci aplikasi yang berisi data sensitif seperti Samsung Pass, Secure Folder, atau Samsung Health.

1. Antisipasi

- Samsung membangun Chain of Trust dari Root of Trust (RoT) perangkat keras tahan rusak

  Root of Trust Samsung tertanam kuat dalam chip dan tidak terpapar dunia luar meskipun hanya dapat diakses oleh serangkaian aplikasi terbatas. Samsung memastikan fungsi perangkat lunak utama kami tidak dirusak saat menawarkan perlindungan data pribadi yang menyeluruh. Fitur keamanan yang didukung perangkat keras memungkinkan pelanggan kami merasa aman dan menjaga ketenangan pikiran.
- Samsung menyediakan lingkungan eksekusi khusus yang memproses data sensitive dan rahasia sekaligus melindungi dari serangan malware

Pemutaran Kembali Video Terlindungi, Autentikasi pengguna, dan Aplikasi Pembayaran berjalan di lingkungan eksekusi kami yang aman. Untuk Aplikasi Autentikasi Pengguna, lingkungan eksekusi aman memblokir akses tanpa izin ke informasi biometrik sensitif. Untuk Aplikasi Pembayaran, lingkungan pelaksanaan kami yang aman memastikan penanganan transaksi pembayaran yang aman.

- Menyimpan data sensitif dalam penyimpanan aman yang terisolasi sepenuhnya

  Data yang sangat sensitif seperti biometrik, nilai PIN, atau PII disimpan dalam penyimpanan aman yang terisolasi sepenuhnya, yang tangguh

terhadap ancaman kebocoran data. Penyimpanan aman kami yang terisolasi sepenuhnya juga tahan terhadap serangan fisik.

- Mengadopsi teknologi kriptografi yang telah terbukti
  Produk dan layanan Samsung menggunakan teknologi kriptografi yang diakui dan distandarkan secara internasional. Kami memastikan penerapan teknologi kriptografi ini melalui sertifikasi seperti Federal Information Processing Standard (FIPS). Data pelanggan disimpan dengan aman dalam bentuk terenkripsi. Mekanisme perlindungan data tersebut juga diterapkan pada data-istirahat dan data-dalam-transit.
- Samsung menerapkan teknologi autentifikasi kuat yang hanya memenuhi syarat pengguna yang ditunjuk untuk mengakses perangkat dan layanan Samsung

Beragam teknologi autentikasi pengguna, seperti PIN, pola, kata sandi, sidik jari, dan pengenalan iris digunakan secara bersamaan untuk menawarkan autentikasi pengguna yang kuat. Selain itu, Samsung Account dapat digunakan untuk mengendalikan akses ke layanan internet, dan multi-otentikasi kami dapat diterapkan agar hanya pengguna yang ditunjuk yang dapat mengakses dan menggunakan perangkat, layanan, dan data

- Samsung secara proaktif membangun mekanisme yang memberi tahu dan memperingatkan pengguna tentang aktivitas ini untuk mencegah potensi ancaman terhadap pengguna
  Samsung mendeteksi dan mencegah upaya perusakan yang diluncurkan pada produk kami untuk memastikan bahwa setiap produk tetap aman dan sehat. Samsung memverifikasi integritas perangkat lunak yang dijalankan pada waktu booting menggunakan booting aman. Teknologi verifikasi perangkat lunak kami mendukung pembaruan perangkat lunak yang mencegah pemasangan pembaruan perangkat lunak yang belum diverifikasi. Teknologi perlindungan waktu nyata kami memberikan perlindungan yang selalu aktif terhadap perangkat lunak waktu aktif dan data sensitif.
- Samsung menerapkan pembaruan dan patch keamanan terbaru untuk memerangi serangan malware dan lanskap peretasan yang terus berubah
  Produk Samsung menyediakan pembaruan keamanan melalui berbagai saluran. Kami menawarkan pembaruan Over-the-Network online serta pembaruan keamanan berkala dan mendesak untuk mengatasi kerentanan secara luas dan cepat.

KESIMPULAN

Kesimpulan sebagai jawaban dari tujuan penelitian berupa intisari dari hasil dan pembahasan penelitian.

REFERENSI

White, P., & MacKenzie, K. (2010). *Deep*
Slimhole Drilling for Geothermal Exploration. Geothermal Resource Council, Vol. 34 2010. Kanada. Referensi dari Prosiding Seminar:
Adityatama, W. Daniel., & Purba, D. (2020).

Slimhole Drilling Overview for Geothermal Exploration in Indonesia: Potential and Challenges. Proceedings The 45th Workshop on Geothermal Reservoir Engineering 2020. California.

Finger, J.T. and Jacobson, R. Slimhole drilling logging and completion technology – an update. Proceedings World Geothermal Congress 2000. Mackenzie, K., Ussher, G., Libbey, R.,

Quinlivan, P., Dacanay, J., & Bogie, I. (2017). *Use of Deep Slimhole Drilling for Geothermal Exploration*. Proceedings The 5th Indonesia International Geothermal Convention & Exhibition (IIGCE) 2017. Jakarta.

Nielson, D., Garg, S., & Goranson, C. (2017).

Slim Hole Drilling and Testing Strategies. Proceedings 6th ITB International Geothermal Workshop (IIGW) 2017. Bandung.