GEBYAR

BULETIN EDISI 49/DESEMBER 2019

AUTO-ID

UNTUK KALANGAN SENDIRI

Ancaman Keamanan Siber Pada Enterprise

Solusi Keamanan Endpoint Yang Mudah Dan Efektif

Tips Aman Ketika
Menggunakan Wi-Fi Publik

MEDIA KOMUNIKASI
PELANGGAN
ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

EDITORIAL

Para pembaca yang budiman dan pelanggan yang terhormat,

Salam sejahtera, Puji syukur pada Tuhan Yang Maha Esa, kita telah mencapai penghujung tahun 2019 ini, semoga semua apa yang telah direncanakan pada tahun 2019 ini telah tercapai sesuai dengan harapan dan menyongsong tahun yang baru 2020 dengan penuh semangat.

Transformasi digital dan industri teknologi hadir dengan berbagai macam teknologi baru, seperti blockchain, artificial Intelligence, dan neural networks. Teknologi ini tersebar ke setiap sektor, mulai dari layanan publik hingga bisnis. Namun keamanan yang dirancang untuk melindungi teknologi baru ini pun masih terbilang sedikit.

Seperti blockchain, telah menciptakan ribuan ide dan bisnis baru tetapi terdapat juga sejumlah peretasan dan serangan. Sama halnya dengan supply chain, yang telah melakukan peningkatan yang luar biasa dalam komunikasi dan presisi, namun tetap berpotensi diretas. Untungnya, keamanan siber terus melaju dengan kecepatan inovasi, dan terdapat banyak solusi baru yang muncul.

Bulletin Gebyar Auto-ID edisi volume yang ke-49/2019 kali ini terbit dengan tulisan mengenai "Ancaman Keamanan Siber Pada Enterprise" yang menyajikan informasi mengenai potensi serangan dan kejahatan siber yang dapat terjadi sewaktu-waktu pada perusahaan serta bagaimana mengantisipasinya. Dan salah satunya adalah dengan solusi keamanan dari DriveLock, vendor IT dari negara Jerman ini berkantor pusat di kota Munich yang telah masuk dalam Top 100 Innovator dengan solusi keamanan yang berprinsip pada Zero Trust platform. Disamping beberapa topik tersebut di atas kami juga menghadirkan informasi lainnya seperti produk highlight, tips & info dan lain-lain. Semoga kehadiran Bulletin Gebyar Auto-ID edisi kali ini dapat memberikan masukan positif dan update informasi yang berguna untuk menunjang kegiatan bisnis dan perusahaan para pembaca semuanya.

Mewakili seluruh tim redaksi bulletin Gebyar Auto-ID, Kami mengucapkan Selamat Hari Raya Natal 2019 kepada para pembaca yang merayakannya, semoga Damai Natal menyertai semua umat dan kebahagiaan senantiasa dirasakan. Dan Selamat Tahun Baru 2020 kepada para pembaca semua, semoga semakin sukses lagi di tahun yang baru, Amin.

Salam Redaksi,
Irvan Kurniawan
Enterprise IT Solutions – Manager
ACS GROUP | PT. Autojaya Idetech - PT. Solusi Periferal

PEMIMPIN REDAKSI
Andre S.Kouanak

SEKRETARIS REDAKSI
Listya Kartikasari (Jakarta)
Indah Widiyanti (Cikarang)
Luh Wayan Sumariani (Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR
Chandra Tjahjadi

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Irvan Kurniawan
Ricky Efraim Lie

ALAMAT REDAKSI
Jakarta (HO)
Perkantoran Gunung Sahari Permai
#C03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.
Telp : +6221-4208221(H), 4205187(H)
Fax : +6221-4207903, 4207904, 4205853

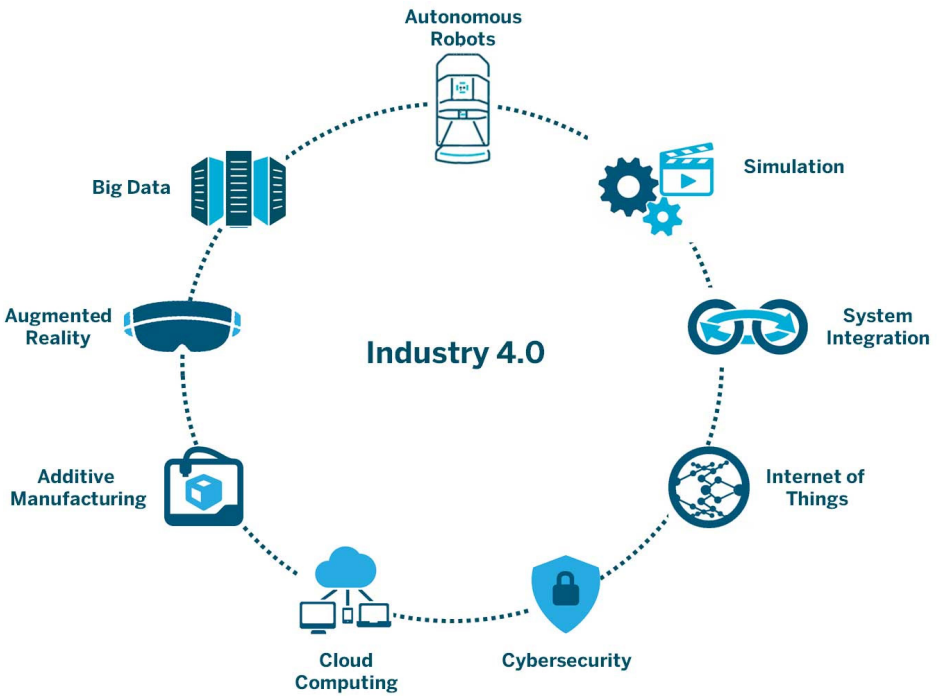
CONTENT

Ancaman Keamanan Siber Pada Enterprise

Keamanan siber sudah menjadi isu global dan mendapat perhatian khusus hampir di semua negara. Keamanan siber sangat penting bagi pertumbuhan bisnis masa depan seiring gencarnya penetrasi teknologi informatika berbasis internet khususnya pada era industri 4.0 saat ini, dimana teknologi manufaktur sudah masuk pada tren otomatisasi dan pertukaran data yang mencakup *cyber physical systems*, *internet of things* - IoT, *cloud computing*, *cognitive computing* dan *artificial intelligence*.

Boston Consulting Group pada 2015 telah mendefinisikan ada sembilan teknologi pendukung Industry 4.0 dan salah satu diantaranya adalah *Cyber Security* atau keamanan siber yang menjadi penopangnya. Berikut gambaran dari sembilan teknologi pendukung dari Industry 4.0:

Cyber Security atau keamanan siber adalah suatu teknologi, proses dan praktik yang dirancang untuk melindungi jaringan komputer, komputer, program dan data dari serangan, kerusakan atau akses yang tidak sah. Istilah "*Cyber Security*" mengacu pada



Gambar 1. Sembilan pilar teknologi pendukung dari Industry 4.0 [1]

Sumber : https://aethon.com/mobile-robots-and-industry4-0/ [1]

fungsi bisnis dan alat teknologi yang digunakan untuk melindungi aset informasi. Data-data perusahaan saat ini telah bertransformasi menjadi data berbasis digital yang digunakan untuk menyimpan, mengakses dan mengambil informasi penting. Melindungi informasi dan data sudah bukan lagi prioritas tetapi sudah menjadi kebutuhan sebagian besar perusahaan dan instansi pemerintah di seluruh dunia. Berdasarkan data **Pusat Operasi Keamanan Siber Nasional tahun 2018**, telah terjadi **232.401.725 serangan siber**[2] sepanjang tahun tersebut. Hal ini berbanding lurus dengan pemanfaatan teknologi informasi dan komunikasi di masyarakat. Selain hal tersebut tingkat resiko dan ancaman serangan siber juga semakin tinggi dan kompleks. "***Cybercrime* di Indonesia tertinggi ke dua di dunia** setelah Jepang. **Total serangan siber ini ada 90 juta**"[3],demikian pernyataan Wakil Kepala Kepolisian Republik Indonesia **Komisaris Jenderal Syafruddin** saat memberikan pidatonya di acara yang diselenggarakan oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) di Jakarta pada Selasa 17 Juli 2019.

perusahaan yang bukan hanya sekadar kerugian finansial dan moneter saja. Dampak dari serangan siber antara lain dapat mengakibatkan berhentinya operasional perusahaan yang berdampak pada produktivitas (47%), **kehilangan kepercayaan pelanggan dan menurunnya reputasi perusahaan (44%),** terhentinya operasional perusahaan yang berdampak terhadap pendapatan (41%), dan berhentinya operasional yang berdampak pada bahaya keselamatan fisik (32%) serta hilangnya potensi bisnis terkait data yang kritis (32%).

Gambar 2. Hasil survey terhadap para Chief Information Security Officer (CISO) mengenai dampak dari serangan siber pada organisasinya

The Bad Actors

Demikian masifnya serangan siber saat ini tentunya menjadi pertanyaan siapa para pelakunya dan apa motifnya. Para pelaku atau peretas ini ada yang menyerang lembaga negara, lembaga finansial, rumah sakit, sekolah dan lembaga lainnya dengan tujuan mencari kepuasan pribadi sampai dengan mencari keuntungan finansial.

Berikut gambaran mengenai lima kategori aktor pelaku serangan siber:

1. **The Explore** : peretas kategori ini melakukan gangguan ataupun serangan siber hanya untuk memenuhi kesenangan dan rasa ingin tahu, ketenaran dan prestise, atau menguji tantangan. Peretas kelompok ini biasanya memiliki sumber daya teknis yang terbatas dan eksploitasi yang dilakukan sudah dikenal sebelumnya. Contoh aksinya seperti *brute force attack* yakni metode untuk meretas password (*password cracking*) dengan cara mencoba semua kemungkinan kombinasi yang ada. Beberapa peretas kelompok ini, jika yang positif akan menginformasikan sebuah celah keamanan kepada si pemilik situs atau sistem sehingga pemilik akan melakukan pembenahan terhadap layanan. Tetapi, ada pula yang memilih untuk tidak memberi tahu celah dan membobol sistem.
2. **Hacktivist** : Kategori ini adalah "Peretas Aktivis" yang beraksi dengan membobol jaringan komputer tertentu untuk mempromosikan sebuah ideologi. Kelompok peretas ini memanfaatkan teknologi untuk mempengaruhi perubahan sosial. Ada yang mempromosikan gerakan kebebasan berbicara, kebebasan berekspresi, hak asasi manusia, sampai kebebasan informasi. Beberapa contoh aksi mereka adalah dengan mengubah tampilan halaman atau situs atau disebut dengan "*deface*" atau melakukan serangan *denial-of-service* (DoS), yang bertujuan untuk membuat berhentinya suatu layanan. Kelompok peretas ini akan berusaha tanpa henti, karena mereka berkomitmen secara emosional dan biasanya memiliki jaringan yang luas dan korban serangannya sudah ditargetkan.
3. **Cyber Terrorist** : Peretas dalam kelompok ini adalah kelompok ekstremis atau aktor non-negara yang menggunakan teknik siber untuk mengintimidasi, memaksa, atau mempengaruhi audiens-nya yang bertujuan untuk memaksakan terjadinya perubahan politik ataupun menyebabkan ketakutan atau kerusakan fisik.

[2] *Sumber : https://www.liputan6.com/news/read/4032955/dpr-diminta-prioritaskan-ruu-keamanan-siber*
[3] *Sumber : https://kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media*

Gambar 3. Kategori aktor pelaku serangan siber [4]

Dalam melakukan aksinya, mereka menyebar program computer yang bersifat merusak atau *malware* ke instansi atau lembaga yang berisi lampiran berbahaya. Jika korban membuka lampiran itu, sistem komputer organisasi akan terinfeksi. *Malware* jenis ini memungkinkan peretas untuk dapat mengunduh, mengunggah, memperbarui, dan menghapus dokumen, dari jarak jauh.

4. **Cyber Criminal** : adalah peretas "Kelompok Kriminal" dimana sebagian besar tujuannya adalah berusaha mencari keuntungan finansial dengan melakukan serangan siber. Sebagian besar penjahat siber ini memang mencari uang dengan melakukan pengelabuan di dunia maya dan ini hal ini telah menjadi tren dalam isu keamanan siber. Contoh aksinya adalah dengan menyebarkan *ransomware* yang dibuat untuk menyandera dokumen pengguna komputer, dan jika pengguna ingin dokumennya kembali, maka mereka harus membayar tebusan dalam bentuk Bitcoin, untuk menjaga agar identitas mereka tetap anonym. *Ransomware* muncul pada tahun 2017 karena dampak luas dari serangan global oleh *WannaCry* dan *NotPetya*. Dan ternyata jumlah serangan *ransomware WannaCry* di Indonesia merupakan jumlah terbanyak kedua di dunia.[5]
5. **Cyber Warrior** : adalah peretas yang terlibat dalam perang siber, baik untuk alasan pribadi atau karena patriotik atau kepercayaan agama, kepentingan nasional suatu negara yang sedang terkait dalam perang siber yang mana para peretasnya membawa misi untuk spionase dan lain-lain. Teknik yang digunakan sudah sangat canggih karena memiliki sumber daya yang hampir tak terbatas dengan serangan yang terus menerus pada tingkat yang lanjut (*advanced persistent threats*). Aktivitas yang

Sumber : Fortinet Network Security Expert 1 Training [4]
Sumber : https://www.liputan6.com/tekno/read/3504303/tak-disangka-serangan-wannacry-di-indonesia-terbanyak-kedua-di-dunia [5]
Sumber : https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack [6]

terjadi pada perang siber ini pada umumnya adalah kegiatan *hacking* dan *anti-hacking* yang dilakukan secara 'resmi' oleh negara. Tujuannya mulai dari mencuri data hingga melumpuhkan sistem yang dimiliki oleh negara musuh. Serangan yang paling serius terjadi tepat sebelum Natal 2015 di Ukraina. Peretas berhasil mengganggu pasokan listrik di beberapa bagian Ukraina dengan menggunakan *Trojan* terkenal yang disebut *Black energy*[6]. Dan berita terakhir menyatakan bahwa *United States Cyber Command* disebut melancarkan sejumlah serangan terhadap infrastruktur listrik milik Rusia selama beberapa bulan sebelumnya [7].

Kejahatan Siber

Badan usaha dan organisasi baik pemerintah dan swasta menjadi target kejahatan siber yang potensial sekarang ini. Hal ini dimungkinkan karena organisasi tersebut kemungkinan tidak memiliki tingkat sumber daya yang sama dalam rangka berinvestasi untuk pertahanan dan keamanan siber mereka. Oleh karena itu, **semua organisasi enterprise sekarang ini harus berasumsi bahwa sistem keamanan jaringan mereka berada dalam kondisi waspada setiap saat.**

Serangan siber adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi.

Beberapa bentuk ancaman siber terkini, yang **Pertama** adalah *ransomware*. ***Ransomware*** masih menjadi salah satu ancaman paling berbahaya dan merugikan. Karakteristiknya adalah melakukan enkripsi terhadap berbagai file penting yang bertujuan membuat korbannya tidak mempunyai pilihan lain selain membayar sejumlah uang tebusan. Hal ini menjadikan *ransomware* menjadi salah satu bisnis yang paling digemari oleh para penjahat siber.

Berdasarkan *Quarterly Threat Landscape Report* dari Fortinet atau laporan mengenai serangan *cyber* per kuartal kedua 2019 (periode April – Juni), dimana insiden terbesar pada kuartal ini menyoroti meningkatnya dampak serangan *ransomware* bagi organisasi atau perusahaan yang tidak siap untuk menghadapinya. Pada bulan Mei 2019 yang lalu, **Baltimore**, kota terbesar di Negara Bagian **Maryland**, Amerika Serikat yang juga tetangga dari kota Washington DC mengalami *ransomware* pada Selasa (7 Mei 2019). Serangan peretas kepada komputer Pemerintah Kota Baltimore ini adalah kali yang kedua dalam setahun terakhir. Akibat dari serangan ini, kota Baltimore mendapati gangguan terhadap beberapa layanan yang kritis selama berminggu-minggu dan memaksa para pejabat untuk mengimplementasikan solusi manual untuk menangani transaksi real estate, pembayaran utilitas, pajak properti, dan fungsi penting lainnya. Pejabat Baltimore, yang bertindak atas saran FBI, menolak untuk membayar sekitar **$ 100.000** (sekitar 1,5 Milyar Rupiah) yang diminta para penyerang sebagai tebusan dan akhirnya menghabiskan lebih dari **$ 18 juta atau sekitar 261 Milyar Rupiah** untuk upaya pemulihan. Dan *ransomware* tersebut adalah: *RobbinHood and Its (Un) Merry Men*.

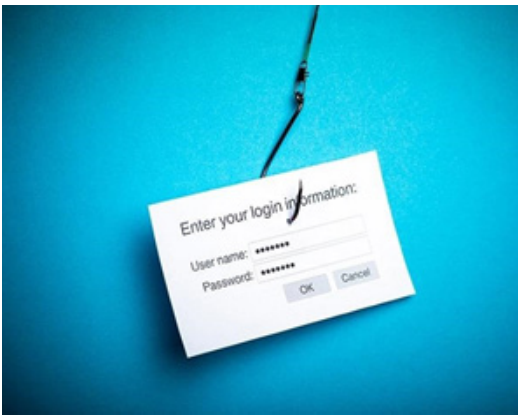
Sementara itu berdasarkan berita **CBS**[8] bahwa serangan *Ransomware* terjadi pada sedikitnya 621 entitas sepanjang tahun 2019 ini hingga bulan September berdasarkan hasil studi terbaru dan targetnya antara lain rumah sakit, pusat kesehatan, sekolah-sekolah dan sejumlah kota dengan menelan biaya kerugian total sekitar $186 juta.

Yang **Kedua**, adalah **Pencurian Data** yang semakin marak dan menjadi korban seperti pencurian data identitas pribadi, dan tampaknya sedikit yang tahu seberapa besar nilai informasi yang dicuri tersebut. Identitas digital yang memuat informasi data pribadi bagi orang tertentu mungkin tidak bernilai banyak jika diuangkan, namun merupakan kunci awal bagi para pelaku kejahatan siber yang dapat digunakan dalam aksinya. Para pelaku kejahatan siber yang melakukan pencurian data dapat melalui akun media sosial dan akses jarak jauh ke server atau desktop, dan bahkan data dari layanan aplikasi populer dan situs *web* untuk permainan yang mungkin menyimpan informasi kartu kredit. Cara yang paling

[7] *Sumber : https://inet.detik.com/cyberlife/d-4588399/pasukan-cyber-as-serang-instalasi-listrik-rusia?_ga=2.222381587.922608636.1569083779-1323923108.1557461257*

[8] *Sumber : https://www.cbsnews.com/news/ransomware-attack-621-hospitals-cities-and-schools-hit-so-far-in-2019/*

umum untuk mencuri data semacam ini adalah melalui kampanye phising spear atau dengan mengeksploitasi kerentanan keamanan dalam perangkat lunak aplikasi. Setelah serangan berlangsung sukses, pelaku akan mendapatkan kumpulan data berisi alamat email, kata sandi untuk layanan yang diretas.



Sementara bagi perusahaan dan organisasi, pencurian data yang terkait data keuangan, informasi pelanggan, kekayaan intelektual, hasil rancangan produk terbaru, atau strategi ekspansi bisnis merupakan aset yang sangat berharga dan akan berdampak buruk apabila jatuh pada oknum-oknum yang tidak bertanggung jawab. Pada tahun 2014 misalnya, pencurian data dalam jumlah sangat besar terjadi pada **Sony Pictures**[9] yang mengakibatkan nilai saham Sony Pictures turun karena banyak data yang dibuka ke publik. Data tentu akan semakin sering bergerak, baik yang tersimpan pada laptop, flash drive, atau bergerak di infrastruktur fisik, virtual, dan *cloud*. **Dan cara mengamankan data di enterprise dapat melalui beberapa hal seperti**:

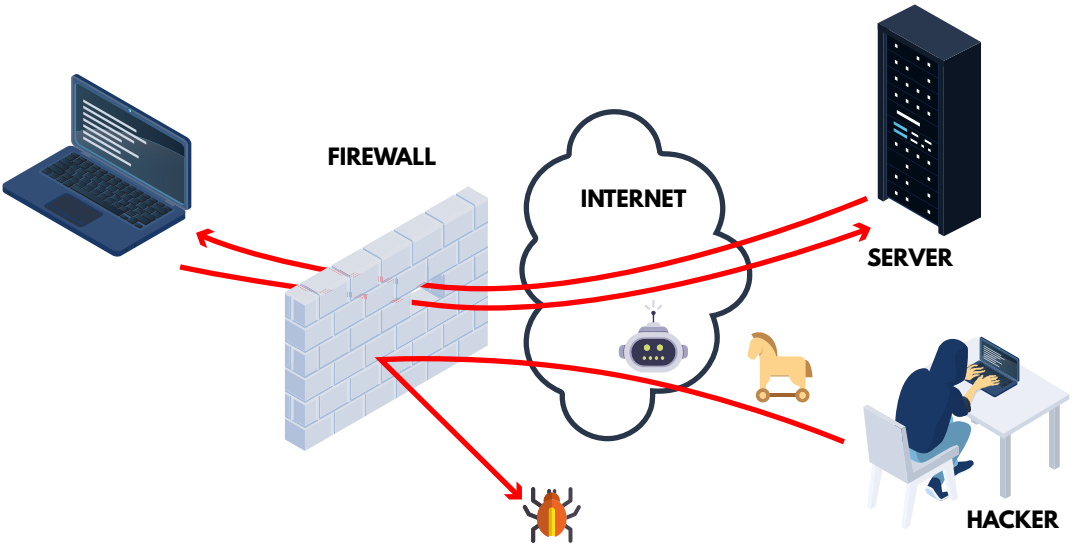
1. Membatasi akses USB *port* dan semua *interface input output* pada perangkat laptop dan desktop karena memiliki beberapa faktor risiko terjadinya pencurian data yang terus meningkat dengan menggunakan media *flash-disk*, *thumb-drive* dan lain sebagainya.
2. Melakukan enkripsi data baik pada disk secara keseluruhan, pada *folder* dan *file* sehingga jika perangkat yang dicuri ataupun hilang, data yang terdapat didalamnya tidak dapat diakses dan dijalankan oleh orang-orang yang tidak bertanggung jawab.
3. Membatasi akses pada aplikasi dan program yang tidak seharusnya pada pengguna terkait operasional sehingga mengurangi resiko terserang *malware* dari aplikasi dan program yang tidak perlu.
4. Melakukan edukasi mengenai keamanan data pada pengguna. Data yang dicuri umumnya karena lemahnya kesadaran pengguna akan keamanan dan cara melakukan perlindungan dari serangan dan faktor-faktor resiko yang mungkin bisa terjadi.

Ketiga, Penyamaran dengan teknik ***social engineering*** merupakan salah satu metode yang telah dirancang dan digunakan oleh peretas untuk memperoleh informasi tentang targetnya, dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai informasi itu. Social engineering mengkonsentrasikan pada rantai terlemah dari sistem jaringan komputer, yaitu **manusia**. Hal ini biasanya terjadi karena lemahnya ***security awareness*** pengguna dimana mudah sekali untuk dibohongi oleh penyerang ataupun dikarenakan faktor kecerobohan dari pengguna. Misalnya dengan modus berpura-pura sedang melakukan survei dari lembaga ternama guna mendapatkan informasi password, akses ke jaringan, peta jaringan, ataupun konfigurasi sistem sebagai pintu awal. Modus lainnya dan banyak terjadi adalah penyamaran sebagai CEO atau direktur keuangan yang memerintah targetnya dengan rancangan suatu situasi yang mendesak dan segera sehingga perlu melakukan perubahan detail pembayaran dan mengalihkan pembayarannya ke akun si penyerang.

Cara yang populer sekarang ini adalah melalui e-mail, dengan mengirim e-mail yang meminta target untuk membuka *attachment* yang telah disisipi *trojan horse* untuk membuat *backdoor* di sistem. *Trojan horse* atau biasa disebut dengan *Trojan* adalah program yang dibuat sepertinya program yang baik dan berguna bagi penggunanya (*crack*, *game*, atau program lainnya yang di-unduh dari *internet*) dan ketika di-*install* ke dalam komputer ternyata menyusupkan kode-kode yang mencurigakan, mencuri data, dan mengirimkan ketukan *keyboard* (*key logger*) ke alamat yang telah ditentukan oleh pembuatnya tanpa diketahui oleh si pengguna komputer tersebut.

Penggunaan istilah *Trojan* atau *Trojan horse*; seperti halnya dalam Perang Troya, para prajurit Sparta bersembunyi di dalam Kuda Troya yang ditujukan sebagai pengabdian kepada Poseidon. Kuda Troya tersebut menurut para petinggi Troya dianggap tidak berbahaya, dan diizinkan masuk ke dalam benteng Troya yang tidak dapat ditembus oleh para prajurit Yunani selama kurang lebih 10 tahun perang Troya bergejolak.

Sumber : https://en.wikipedia.org/wiki/Sony_Pictures_hack [9]



Keempat, bentuk kejahatan siber yang relatif baru tetapi semakin banyak terjadi adalah ***Cryptojacking*** untuk keperluan penambangan mata uang kripto (*bitcoin* dan mata uang kripto lainnya). *Bitcoin* masih menjadi incaran karena nilai tukarnya yang tinggi dan dapat ditambang secara digital. Komputer yang telah terkena serangan *malware* secara diam-diam akan "dimanfaatkan" untuk menambang mata uang kripto, proses "menumpang" dan membajak sumber daya prosesor pada komputer korban untuk menambah kekuatan pemrosesan komputer sehingga menghasilkan koin baru yang berpotensi menguntungkan si penyerang. Insiden *malware* yang mengandung alat penambangan kripto (*crypto-mining*) telah meningkat enam kali lipat tahun ini, menurut IBM Managed Security Services[10].

Serangan cryptojacking sangat meningkat pada kuartal kedua 2019. Jenis *malware* yang digunakan dalam cryptojacking, antara lain: XMRig, CoinHive, dan CoinMiner. Yang paling banyak digunakan adalah XMRig (62%). Kekhawatiran CryptoJacking semakin nyata dimana menyerang secara besar-besaran ke

[10] *Sumber : https://www.infosecurity-magazine.com/news/ibm-cryptomining-attacks-increased/*

seluruh dunia yang menargetkan perangkat router, khususnya perangkat router consumer dimana pelaku memanfaatkan kerentanan lama, yang tidak dilakukan patching pada perangkat router korban. Dengan kerentanan tersebut peretas dapat menggunakan akses dan mengubah konfigurasi yang kemudian menyuntikkan skrip penambangan cryptocurrency Coinhive atau *Crypto-Loot* di *web browser* para pengguna.

Terakhir, kejahatan pencurian Intellectual Property (IP) seperti hak cipta, rahasia dagang, paten dan lain sebagainya dengan metode pencurian yang terjadi melalui internet dan komputer. Hal ini biasanya terjadi dengan modus spionase industri yang telah menargetkan sistem perusahaan saingan untuk mencuri intellectual property. Kompetitor yang ambisius merasa jauh lebih cepat dan lebih murah daripada berinvestasi untuk berinovasi dari awal serta biaya penelitian dan pengembangan (R&D) yang meningkat, sementara peluang pasar menyusut menyebabkan meningkatnya insiden pencurian intellectual property.

Kehilangan data pelanggan oleh peretas bisa sangat mahal ongkosnya dan juga memalukan, tetapi dengan kehilangan kekayaan intelektual oleh para pencuri di dunia maya akan mengancam masa depan perusahaan. Oleh karenanya, langkah pertama yang dapat dilakukan perusahaan adalah memprioritaskan perlindungan terhadap intelektual propertinya dan kesiapan dalam mencegah dan mengantisipasi dari kemungkinan insiden. Memulai konsultasi dengan pakar sistem keamanan dan menguji adanya kerentananan pada sistem keamanan perusahaan atau biasanya dikenal dengan istilah penetration test. Sehingga didapatkan penilaian yang tepat mengenai perlu tidaknya tindakan korektif ataupun tindakan preventif guna mencegah kemungkinan kerugian dari pencurian intellectual property yang makin marak terjadi.

Saran dan Penutup

Dengan terus meningkatnya serangan dan kejahatannya siber, aspek manajemen keamanan siber perlu mendapat perhatian yang sama seperti pada bagian lain dari organisasi enterprise dan SMB. Risiko telah tumbuh dan harus dapat ditangani dengan tepat. Langkah-langkah awal untuk rencana manajemen risiko terkait keamanan siber dapat dimulai dengan:

1.) Identifikasi risiko,

2.) Menganalisis risiko (mengukur frekuensi dan tingkat *severity*),

3.) Mengevaluasi risiko (mencari alternatif),

4.) Penanganan risiko (strategi dalam menghadapi ancaman dan peluang)

5.) Pantau dan tinjau bagaimana manajemen risiko berjalan dan beradaptasi sesuai kebutuhan.

Strategi keamanan siber dalam enterprise tentunya terkait dengan tim dan sumber daya yang ahli serta individu yang berpengalaman dalam merancang sistem keamanan itu sendiri serta kapabiltas dalam mengantisipasi dan menghadapi serangan siber dan hal ini membutuhkan waktu dan investasi dalam proses perekrutan dan pengembangan.

Memahami akan hal tersebut dan agar terjadinya akselarasi, maka tim *security* ACS Group bersama dengan tim distributor menghadirkan layanan konsultasi keamanan siber dengan paket konsultasi yang sangat terjangkau sehingga memungkinkan untuk akses dan konsultasi ke *Certified Professional* Keamanan Siber dan praktisi keamanan siber yang telah berpengalaman rata-rata di atas 5 tahun yang dapat mendiskusikan beberapa strategi untuk mencapai tujuan menyeluruh guna meningkatkan keamanan dan kelangsungan bisnis di Enterprise dan SMB.

Dan dengan layanan premier, Anda akan mendapatkan laporan mengenai *Initial Threat Assessment report* pada organisasi Anda dari perspektif peretas serta saran dari Konsultan untuk mengurangi potensi resiko keamanan yang teridentifikasi.

Segera hubungi team ACS Group untuk informasi lebih lanjut mengenai layanan keamanan siber ini.

*/ Penulis : Irvan Kurniawan(irvan@acsgroup.co.id)

Solusi Keamanan Endpoint Yang Mudah Dan Efektif

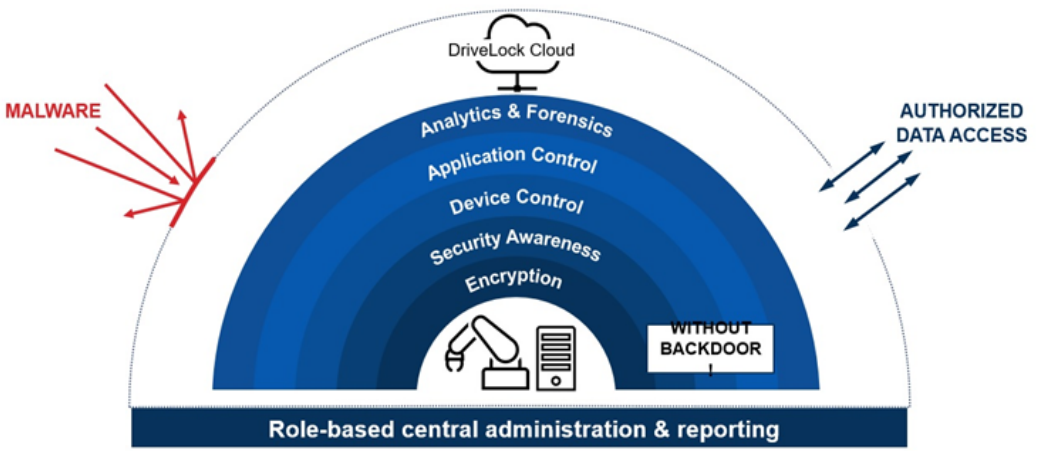
Mengamankan jaringan adalah sebuah usaha yang memiliki kompleksitas khususnya dalam jaringan komputer karena ada banyak sekali faktor yang berpengaruh dan perlu dilindungi. Hal utama yang biasanya terlintas ketika berbicara keamanan jaringan adalah sebuah perangkat *network firewall*, tetapi sayangnya perangkat *network firewall* tidak kedap mengamankan 100% jaringan dari berbagai *malware* dan serangan, terutama jika serangan masuk bukan melalui gerbang jaringan atau biasa disebut gateway yang menghubungkan jaringan internal dengan jaringan internet seperti pada umumnya perangkat *network firewall* diposisikan.

Dua serangan yang sering kali terjadi adalah email *phising* dan *malware* yang masuk melalui komputer pengguna adalah *USB flash drive*, *CD-ROM*, HDD eksternal, dan lain sejenisnya merupakan hal yang tidak dapat dikendalikan oleh perangkat *network firewall* tetapi membutuhkan perlindungan khusus dengan menggunakan pengamanan *endpoint security* atau aplikasi pengamanan pada komputer pengguna.

Terdapat banyak aplikasi *endpoint security* di pasaran yang memiliki fitur yang beragam seperti antivirus, *endpoint firewall*, *anti-malware*, *anti-spyware*, *encryption software*, dan lain-lain. Tetapi dari begitu banyaknya fitur, ada hal-hal mendasar yang tidak bisa diamankan oleh banyak aplikasi tersebut yaitu kemampuan enkripsi yang memadai, kemampuan pengendalian perangkat yang terkoneksi ke komputer tersebut, edukasi kepada para pengguna untuk terbangunnya sistem keamanan yang baik, dan lain-lain.

Hal inilah dibutuhkannya aplikasi keamanan dari DriveLock sebagai solusi *endpoint* security. DriveLock adalah software dengan solusi keamanan "*Next Generation*" yang mampu memberikan perlindungan secara berlapis dan menyeluruh dengan pilihan modul yang fleksibel serta didukung integrasi penuh dengan *Active Directory* yang dapat dikelola dengan manajemen terpusat (*centralize management*) dengan *Console Management*-nya. Saat ini, aplikasi DriveLock telah digunakan di lebih dari 30 negara dengan pelanggan dari berbagai industri termasuk sektor keuangan, kesehatan, manufaktur, badan pemerintahan dan sektor lainnya.

DriveLock dikembangkan di Jerman, adalah perangkat lunak keamanan data dan merupakan solusi tanpa "*back-doors*" yang sangat taat dan patuh mengikuti

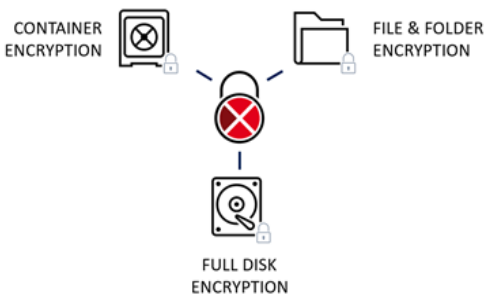


standar peraturan perlindungan data dan perangkat yang berlaku dengan konsep keamanan multi-layer. Banyak solusi keamanan data sekarang ini namun terlalu rumit dan tidak efisien, sehingga menimbulkan biaya yang tidak perlu dan menghambat produktivitas. DriveLock mempunyai lima fitur utama yang akan kita bahas satu persatu.

1. ***Encryption***

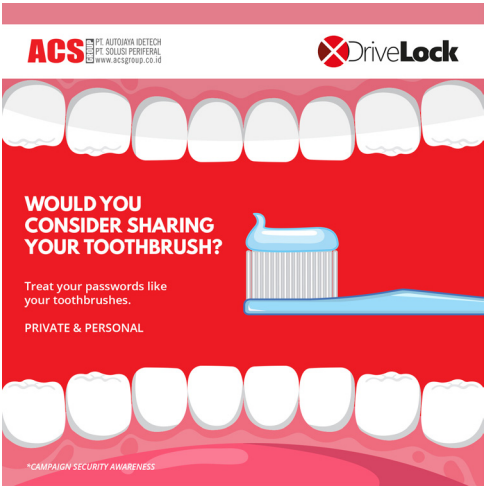
   Encryption atau enkripsi adalah fitur untuk meng-kode-kan atau mengacak cara sebuah komputer menyimpan sebuah data agar data tersebut tidak dapat diakses dan dibaca oleh orang lain yang tidak diijinkan (*authorized*). Teknik enkripsi yang digunakan pada DriveLock adalah menggunakan teknologi militer tingkat tinggi yang dilengkapi otentikasi sebelum proses booting (*Pre-Boot Authentication* untuk BIOS dan UEFI) untuk memberikan otentikasi masuk ke komputer menggantikan windows logon agar lebih aman.

   Fleksibilitas enkripsi DriveLock sangat baik karena dapat diterapkan pada level folder, USB Drive, ataupun keseluruhan HDD untuk melindungi komputer secara keseluruhan. Dan apabila perusahaan sudah menggunakan aplikasi BitLocker maka DriveLock dapat diterapkan sebagai *centralized* management untuk mengatur *key* dari semua aplikasi BitLocker tersebut.



2. ***Security Awareness***

   Banyak sekali potensi serangan *malware* dapat dihindari apabila pengguna memiliki pengetahuan dan kesadaran terhadap keamanan, karena para pengguna adalah pertahanan terakhir dalam sistem pengamanan. Fitur *Security Awareness* dari DriveLock adalah sebuah *campaign* yang dapat diberikan oleh perusahaan ke semua pengguna untuk meningkatkan kesadaran tentang keamanan jaringan dan hal lainnya yang berhubungan.



Campaign yang dimaksud dapat berupa gambar, video, kuliah singkat, ataupun layar interaktif tanya jawab (*quiz*) yang harus dijalankan oleh pengguna setiap saat ingin menggunakan komputer seperti pada waktu pagi hari. Diharapkan dengan *campaign* ini setiap pengguna memiliki pengetahuan dan kesadaran yang tinggi terhadap keamanan dan tidak menjadi lalai terhadap potensi serangan yang mungkin timbul serta pada akhirnya meningkatkan produktivitas di perusahaan dengan tidak terjadinya gangguan pada operasional.

3. *Drive & Device Control*

Banyak serangan yang mungkin terjadi secara tidak sengaja oleh para pengguna sendiri dimana yang paling sederhana adalah penggunaan sebuah Flash Disk atau Flash Drive yang tidak mempertimbangkan aspek keamanannya. Flash Drive yang sudah pernah terhubung dengan komputer non-perusahaan memiliki potensi sangat besar disusupi oleh *malware* dan ketika flash drive tersebut terhubung dengan komputer perusahaan maka dengan sangat mudah *malware* yang ada di flash drive tersebut untuk segera menyebar. Hal sederhana lainnya dapat juga terjadi pada flash drive yang digunakan secara internal untuk menyimpan atau bertukar data yang sensitif dimana mengandung unsur kerahasiaan akan sangat riskan apakah hilang atau terjatuh dan ditemukan oleh pihak yang tidak bertanggung jawab.

Holistic drive & device control including BadUSB protection

Fitur *Drive & Device Control* mengamankan perangkat tersebut dengan membatasi Flash Drive yang dapat terkoneksi karena memiliki kemampuan untuk mengidentifikasi dari serial number, Part Number, jenis Flash Drive dan lain-lain. Untuk memastikan bahwa hanya flash drive tertentu yang dapat digunakan atau bahkan melakukan proses enkripsi agar apabila flash drive tersebut terjatuh dan hilang maka data yang terdapat di dalamnya tetap aman dan tidak dapat terbaca oleh sembarang orang.

Pada contoh penggunaan lainnya adalah pengamanan terhadap perangkat PC atau desktop komputer yang digunakan untuk operasional perusahaan seperti pada mesin ATM, *Point of Sales* (POS), *kiosk*, mesin industri dan lain sebagainya haruslah dipertimbangkan pengamanannya dengan membatasi perangkat yang dapat terhubung. Mesin-mesin tersebut dapat terhubung dengan *mouse*, *keyboard*, *printer*, *scanner barcode*, dan lain-lain bahkan dengan *smartphone* untuk keperluan *file sharing*, sehingga harus dipastikan bahwa port *interface* yang terhubung adalah untuk keperluan yang memang seharusnya dalam operasional.

4. *Application Control*

Fitur *Application Control* ini mirip seperti fungsi *firewall Application Visibility Control* (AVC) ataupun *Deep Packet Inspection* (DPI) dimana fungsi intinya adalah memonitor *traffic* atau lalu-lintas jaringan untuk mengetahui aplikasi apa yang digunakan pengguna dan melakukan blokir untuk aplikasi yang tidak sesuai kebijakan perusahaan. Tetapi pada perangkat *firewall* tidak sepenuhnya dapat mengamankan perangkat, seperti contoh beberapa hal berikut ini:

a. Perangkat *firewall* hanya dapat memeriksa apabila *traffic* yang menuju ke dan dari internet yang dilindungi oleh perangkat *firewall*, tentu menjadi pertanyaan bagaimana bila aplikasi hanya berjalan pada lokal jaringan saja? Kemungkinan lainnya adalah apabila komputer pengguna mengakses internet melalui jaringan lain seperti pada saat berada di café atau area publik, atau melakukan tethering, dan berpotensi membawa malware.

b. Perangkat *firewall* hanya mengamankan pada sisi gateway atau pada pintu gerbang jaringan dan aplikasi dapat terus berusaha mengirimkan paket data yang terus menerus sehingga dapat membebani lalu-lintas jaringan, perangkat *firewall* tidak dapat melakukan blokir dari sumbernya.

c. Perangkat *firewall* belum tentu memiliki kemampuan untuk pemeriksaan dan pemblokiran terhadap paket data yang sudah terenkripsi seperti HTTPS karena paket ini tidak dapat secara keseluruhan dikenali karena sudah mengalami proses enkripsi.

Dengan adanya beberapa kemungkinan celah keamanan tersebut di atas, maka pengamanan *endpoint protection* seperti DriveLock sangat diperlukan karena DriveLock melakukan pemblokiran di lokal komputer sehingga langsung dinon-aktifikan dari sumbernya sebelum aplikasi tersebut dapat

mengirimkan data melalui jaringan. Pemblokiran dilakukan terhadap aplikasi itu sendiri dan bukan terhadap data yang dikirimkan oleh aplikasi sehingga enkripsi yang dilakukan oleh aplikasi tidak akan ada pengaruhnya lagi.

5. ***Analytics and Forensic***

Fitur terakhir adalah untuk perusahaan atau administrator agar dapat melakukan analisa kegiatan komputer yang dilakukan oleh pengguna seperti *file* apa yang dibuka oleh pengguna, Flash Drive yang digunakan oleh pengguna, bahkan sampai pada *file* perusahaan yang di-*copy*-kan ke Flash Drive. DriveLock melakukan pelacakan terhadap kegiatan pengguna dan melakukan pembuatan laporan secara khusus dan mengirimkannya secara berkala.

DriveLock juga menawarkan sistem pemantauan yang dapat mengurutkan dan melacak bagaimana lalu-lintas *file* berlangsung untuk mendapatkan tinjauan bagaimana pelanggaran keamanan terjadi. DriveLock merinci komputer mana, pengguna mana dan aplikasi mana yang terjadi pelanggaran data dan investigasi terhadap insiden ini dilakukan secara otomatis.

Berikut beberapa contoh laporan yang dihasilkan:

Report: File events 10.10.2019 17:36

Report: File events

Displays all file events.

Type [Events]	Description [Events]	Event ID [Events]	User [Events]	Computer name [Events]	Date / Time [Events]	File name [Files]	File extension	File size [Files]	Access direction	Process name	HW Vendor ID [Drives]	HW Product ID [Drives]
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:59 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:59 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade
Audit failure	File extension blocked	148	ACSLAB\putra	PUTRA	10/2/2019 11:31:58 AM	asoy.jpg	jpg	973 KB	Read	C:\Windows\System32\sihost.exe	SanDisk	Cruzer Blade

1/6

Report: Drive events 10.10.2019 17:08

Report: Drive events

Displays all drive events.

Type [Events]	Description [Events]	Event ID [Events]	User [Events]	Computer name [Events]	Date / Time [Events]	Drive letter	User locking state	Drive type [Drives]	Storage bus type [Drives]	HW Vendor ID [Drives]
Audit success	Drive locked	115	ACSLAB\ADTest 02	DESKTOP02	10/8/2019 1:29:14 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive connected and unlocked	110	ACSLAB\ADTest 02	DESKTOP02	10/8/2019 1:29:08 PM	C:\	not locked	Hard disk	SAS	VMware
Audit success	Drive locked	115		DESKTOP02	10/8/2019 1:28:57 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive locked	115	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 2:53:09 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive connected and unlocked	110	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 2:53:01 PM	C:\	not locked	Hard disk	SAS	VMware
Audit success	Drive locked	115		DESKTOP02	10/3/2019 2:52:42 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive connected and unlocked	110		DESKTOP02	10/3/2019 2:51:34 PM	C:\	not locked	Hard disk	SAS	VMware
Audit success	Drive locked	115		DESKTOP02	10/3/2019 2:51:34 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive locked	115	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 2:47:43 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive connected and unlocked	110	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 2:47:35 PM	C:\	not locked	Hard disk	SAS	VMware
Audit success	Drive locked	115		DESKTOP02	10/3/2019 2:42:11 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive connected and unlocked	110		DESKTOP02	10/3/2019 2:38:51 PM	C:\	not locked	Hard disk	SAS	VMware
Audit success	Drive locked	115		DESKTOP02	10/3/2019 2:38:51 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive locked	115	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 2:38:18 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive locked	115	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 2:18:51 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive locked	115	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 2:01:04 PM	D:\	locked	CD-ROM	SATA	NECVMWar
Audit success	Drive locked	115	ACSLAB\ADTest 02	DESKTOP02	10/3/2019 1:49:57 PM	D:\	locked	CD-ROM	SATA	NECVMWar

1/4

Pada mesin keamanan DriveLock, menyediakan utilitas yang mudah digunakan dan dapat dikonfigurasi cepat, tepat, fleksibel menyesuaikannya dengan situasi yang relevan. Hal ini memungkinkan tingkat perlindungan keamanan yang handal dan mendapatkan manfaat yang luar biasa.

Dengan konsep keamanan yang disesuaikan dengan persyaratan yang tepat dari masing-masing perusahaan, DriveLock memberikan perlindungan yang luas – terhadap ancaman internal dan eksternal – tanpa mempengaruhi efisiensi proses kerja. Dengan cara ini, perusahaan dapat menyelaraskan tujuan strategisnya dalam mencapai tujuan keamanan pada organisasinya dan mendorong bisnis mereka lebih maju lagi ke depan.

*/ Penulis : Ricky Efraim Lie(ricky.lie@acsgroup.co.id)

Hadiah Natal Berupa e-Money

KOLOM KETAWA

Seorang kakek memutuskan bahwa membeli hadiah Natal akan sangat merepotkan dan sulit, karena semua cucunya yang ada di luar kota sudah memiliki semua yang mereka butuhkan, jadi dia memutuskan untuk mengirim mereka masing-masing sebuah kartu Natal dan e-Money dengan saldo setiap kartu adalah 1 juta.

Di setiap kartu Natal ia menulis:

"Selamat Natal dari Kakek. Oh ya, beli hadiahmu sendiri ya!"

Pada awal tahun berikutnya, saat Kakek mengadakan acara keluarga di rumahnya yang dihadiri oleh seluruh anak dan cucu. Saat itulah, si kakek mulai merasa bahwa cucu-cucunya sedikit menjauh darinya. Si kakek mulai berpikir apakah hal itu karena hadiah Natalnya berupa uang.

Kemudian suatu hari si kakek mulai bersih-bersih rumah memilah-milah barangnya dan di bawah tumpukan majalah, dia menemukan setumpuk kartu e-Money untuk cucu-cucunya. Ternyata si kakek benar-benar lupa memasukkan e-Money itu di amplop kartu Natal yang telah dia kirimkan untuk cucu-cucunya.

Launching

LAUNCHING ARUBA INSTANT ON DI LOMBOK-NTB

ACS Group bersama PT Sistech Kharisma yang merupakan disti HPE Aruba dan Komunitas Profesional IT Lombok (PROFIT) melaunching Aruba Instant On untuk wilayah NTB pada tanggal 5 Oktober 2019. Merupakan salah satu bentuk dukungan perkembangan pariwisata di daerah ini. Hadirnya Aruba Instant On sebagai solusi WiFi sederhana dan aman untuk industri hospitality yang sedang berkembang di NTB seperti perhotelan, restoran dan fasilitas umum. Sebagai daerah pariwisata yang sering dikunjungi oleh wisatawan manca negara maupun lokal, keamanan dan kenyamanan penggunaan WIFI merupakan syarat mutlak yang harus dipenuhi oleh para pebisnis di industri ini.

Instant On memadukan teknologi Wi-Fi kelas bisnis dari Aruba dengan solusi yang sederhana, mudah diimplementasikan, dan menawarkan fleksibilitas sehingga bisa terus ditingkatkan kapasitasnya sesuai dengan kebutuhan bisnis. Aruba sendiri sebuah perusahaan Hewlett Packard Enterprise yang hadir dengan solusi jaringan nirkabel terbaru aman dan kuat. ”Solusi Aruba Instant On mudah diimplemantasikan, hemat biaya, dapat terus ditingkatkan kapasitasnya, dan yang pasti keamanannya.

Join Event

KERJASAMA ACS GROUP DENGAN ASOSIASI IT HOSPITALITY INDONESIA

HITA Kalimantan Timur (Balikpapan)

ACS Group beberapa tahun belakangan ini melakukan kerjasama dengan beberapa asosiasi IT hospitality di Indonesia. Di bulan Oktober dan November 2019 kali ini bekerjasama dengan HITA (Hotel Information Technology Association) dan CITAH (Hospitality Information Technology Cikarang-Karawang).

HITA Balikpapan menggelar acara pelatihan dan sharing Perkembangan Teknologi Industry 4.0 pada tanggal 19 Oktober 2019. Acara ini diselenggarakan agar para anggota memperoleh update teknologi IT di Industri hospitality. Dalam acara ini ACS Group bersama Honeywell Security turut serta berpartisipasi sebagai salah satu sponsor di HITA Balikpapan sekaligus

memperoleh kesempatan untuk membuka wawasan para anggota yang hadir dalam presentasi mengenai "Security System Solutions - Honeywell Building Technology'. Cakupan pada tahap awal sistem keamanan diperlukan pendeteksian dari kejauhan sebelum sesuatu terjadi, setelah terdeteksi maka masih bisa masuk, namun tentunya akan diproteksi dan system akan langsung memberikan alert ke surveilance.

Selanjutnya berpartisipasi sebagai sponsor dan mitra teknologi industri pada acara seminar pendidikan oleh HITA Jawa Tengah yang dilaksanakan di kota Solo pada tanggal 5 November 2019, dihadiri sekitar 100 anggota organisasi HITA dari wilayah Jakarta, Yogyakarta, Solo, Jawa Tengah dan Jawa Barat. Pada acara ini ACS Group bersama HPE Aruba menyampaikan "Mobile First for Hospitality", teknologi Aruba yang menawarkan beragam solusi salah satunya adalah solusi "Hotel Pintar" yang memungkinkan pelanggan hotel untuk check-in dan langsung menuju pintu kamarnya tanpa harus antri di resepsionis hotel. Dan fitur penunjuk jalan atau GPS dalam ruang memungkinkan pelanggan hotel menuju spot-spot yang ingin dituju dalam area hotel. Disamping itu pengenalan akan solusi Aruba Instant On sebagai solusi sederhana yang sangat mudah diimplementasikan, hemat biaya serta fleksibilitas yang mumpuni sehingga dapat ditingkatkan kapasitasnya sesuai dengan kebutuhan bisnis.

Sedangkan di Acara CITAH yang berlangsung di Swisbell In Hotel - Karawang, ACS Group bersama HPE Aruba dan Honeywell Security juga menyampaikan solusi yang sama yaitu "Mobile First for Hospitality" dari Honeywell Security dan solusi Aruba Instant On dari HPE Aruba.

ACS Group siap membantu dan bermitra dengan perusahaan anda dalam mengimplementasikan solusi kami yang sudah terbukti, hubungi kami segera.


HITA Kalimantan Timur (Balikpapan)

HITA Jawa Tengah (Solo)


HITA Jawa Tengah (Solo)


CITAH Cikarang


CITAH Cikarang

FORTINET
FortiSandbox-500F

Solusi untuk sektor industri : Semua sektor industri.

Untuk mengakomodir mid-size market, Fortinet memperkenalkan solusi Fabric-enabled entry level sandbox yakni FortiSandbox-500F. Semua skala bisnis membutuhkan advanced threat protection –ATP dalam menghadapi volume serangan siber yang semakin massive dan sophisticated. Dengan FortiSandbox-500F, menjawab kebutuhan akan affordable advanced threat protection dimana pada mid-size business yang terbatas security resources dan tight budget, dan perangkat ini memiliki kapabilitas yang secara automasi menangani sejumlah proses terhadap manajemen serangan atau threat management cycle seperti prevention, detection hingga mitigation.

NSS Labs merekomendasikan Fortinet Sandbox sebagai Advanced Threat Protection - ATP solution dengan beberapa portfolio produk Fortinet lainnya.

FortiSandbox-500F memiliki Form Factor 1 RU untuk hardware appliance-nya dengan kinerja Effective real-world throughput (files/hr) = 200 (upgradeable to 600) dan terdapat Ports 4x GE RJ45 ports.

FORTINET
FortiGate: Next-Generation Firewall

Solusi untuk sektor industri : Semua sektor industri.

Disebut dengan "Next-Generation Firewall" (NGFW) karena sistem firewall-nya bukan perangkat firewall tradisional yang hanya menyaring lalu lintas jaringan yang menggunakan alamat IP, nomor port, dan protokol, tetapi hadir dengan fungsi dan kontrol yang lengkap untuk menghadapi dan mengatasi resiko ancaman dan serangan akan keamanan data terbaru.

Beberapa manfaat dan fungsi yang didapatkan dari perangkat FortiGate Next Generation Firewall adalah sebagai berikut:

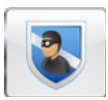
1. **ACCERELATED FIREWALL IPV4 IPV6**

Sistem keamanan yang memantau dan mengontrol lalulintas data baik yang keluar dan yang masuk ke dalam jaringan sesuati dengan aturan keamanan yang telah ditentukan. Firewall ini telah diakselerasi dan dapat berjalan di protokol IP Address versi 4 (IPv4) dan protokol IP Address versi 6 (IPv6).

2. **ANTI VIRUS & ANTI BOTNET**

Mendeteksi dan menghapus virus yang mengancam jaringan serta BOTNET yang berasal dari dua kata, robot dan network, merupakan sebuah robot yang mengendalikan dari jarak jauh setelah masuk dalam jaringan dan menciptakan serangan DDoS (Distributed Denial of Service) sehingga menyebabkan berhenti layanan sistem informasi.

3. **INTRUSION PROTECTION SYSTEM & INTRUSION DETECTION SYSTEM – IPS & IDS**



Menyertakan fitur intrusion prevention dan detection yang powerful, dengan tidak hanya melihat port dan protokol yang digunakan tetapi hingga konten aktual pada lalulintas jaringan dan mengidentifikasi serta menghentikan ancaman-ancaman keamanan yang mungkin terjadi karena adanya kapabilitas pembacaan paket secara mendalam (deep packet scanning).

4. **ANTI SPAM**

Antispam sangat efektif dan kunci untuk melindungi organisasi dari serangan karena email adalah vektor pertama untuk memulai serangan lanjutan pada suatu organisasi. FortiGuard Antispam menyediakan pendekatan yang komprehensif dan berlapis-lapis untuk mendeteksi dan memfilter spam. Teknologi pendeteksian dual-pass-nya dapat secara dramatis mengurangi volume spam di area perimeter.

5. **DYNAMIC WEB FILTERING**

Mengatur dan membatasi akses ke situs internet tertentu dan kemampuan mendeteksi situs yang berbahaya dan situs yang tidak pantas (inappropriate website). Web filtering yang dinamis, mencakup lebih dari 250

juta situs website yang mana terdapat 1,5 juta situs website baru setiap minggunya.

Melindungi dan mem-block akses ke situs yang malicious, hacked, dan inappropriate websites yang berpontensi memberikan ancaman dengan mengunduh malware, spyware, dan konten yang berisiko.

6. APPLICATION CONTROL

Dengan adanya application control, maka dapat dengan cepat membuat kebijakan untuk mengizinkan, menolak, atau membatasi akses ke aplikasi atau seluruh kategori aplikasi.

Menyediakan secara komprehensif, visibilitas dan kontrol atas lebih dari 3000 jenis aplikasi 3rd party untuk enforcement/penegakan kebijakan-kebijakan perusahaan yang sesuai dengan user maupun device-based profile-nya.

7. SSL & IPSec VPN (+ADVPN)

FortiGate dengan Crypto VPN (enkripsi aman yang melindungi dan memverifikasi), skalabiltas dan berkinerja tinggi untuk melindungi pengguna dari serangan man-in-the-middle dan data breach. Teknologi Fortinet VPN menyediakan komunikasi yang aman di Internet antara beberapa jaringan dan endpoint melalui teknologi IPsec dan Secure Socket Layer (SSL). Prosesor FortiASIC-nya meningkatkan akselerasi dari perangkat keras untuk menyediakan komunikasi berkinerja tinggi dan menjaga privasi data.

8. TRAFFIC SHAPPING & QOS (QUALITY OF SERVICE)

FortiGate memberikan QoS dengan menerapkan batas bandwidth dan prioritas. Dengan Traffic shaping akan dapat menyesuaikan bagaimana FortiGate mengalokasikan sumber daya ke berbagai jenis lalu lintas untuk meningkatkan kinerja dan stabilitas aplikasi jaringan terhadap latency sensitive dan bandwidth intensive.

9. LINK LOAD BALANCING

Menjaga ketersediaan internet dan membagi beban akses internet dengan menggunakan dua atau lebih Internet Service Provider (ISP).

Serangan seperti Zero-day, advanced targeted attacks, ransomware, polymorphic malware dan distributed denial-of-service (DDOS) attacks dapat diatasi Fortinet next-generation firewall (NGFW) yang sudah built IPS technology lebih dari 10 tahun.

DRIVELOCK
DriveLock Smart AppProtect

Solusi untuk sektor industri : Semua sektor industri.

Hadir dengan solusi yang holistik dan tanpa back-door dengan modul-modul

1. Encryption untuk melakukan enkrispsi data baik terhadap file, folder hingga full-disk
2. Security awareness untuk kampanye mengenai keamanan dalam mengedukasi pengguna
3. Device Control untuk meng-otorisasi interface perangkat sesuai pada peruntukan dan penggunaannya
4. Application Control untuk melakukan whitelist terhadap aplikasi-aplikasi yang dapat dijalankan atau yang diperbolehkan di endpoint
5. Analytics & Forensics untuk melacak bagaimana pelanggaran keamanan terjadi dan investigasi terhadap insiden ini dilakukan secara otomatis.

Untuk penjelasan lebih detail lagi anda dapat menghubungi fitur chat kami di www.acsgroup.co.id.

INGRAM MICRO
Cybersecurity Advisory CMAS Services

Solusi untuk sektor industri : Semua sektor industri

BASIC SMB

Cyber Security Advisory Base Service

- Guarantee access to certified Security Professional
- Entitled upto 4 hours of Professional time whether onsite or offsite
- 8x5 phone line or email access, excluding weekends adn public holidays
- 4 hours response time via call or 1 business day via email

PREMIER SMB

Cyber Security Advisory Base Service

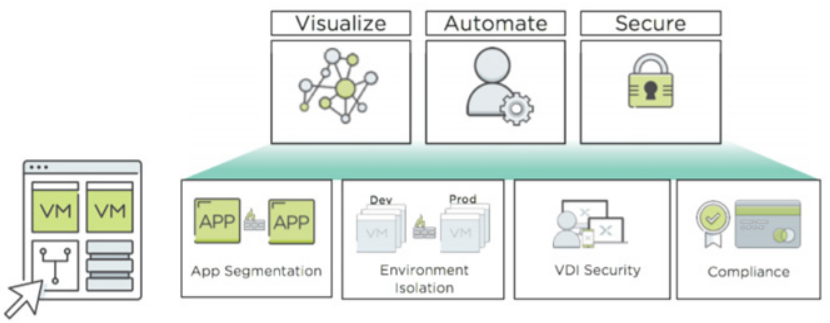
- Guarantee access to certified Security Professional
- Entitled upto 4 hours of Professional time whether onsite or offsite
- 8x5 phone line or email access, excluding weekends adn public holidays
- 4 hours response time via call or 1 business day via email
- Initial Threat Assessment Report against organization's exposed security related information & vulnerabilities that are known to hackers
- Advice against this Initial Threat Assessment Report
- Yearly Cyber Threat landscape sharing event

NUTANIX
NUTANIX FLOW

Solusi untuk sektor industri : Semua sektor industri.

Nutanix Flow hadir memberikan layanan keamanan dan jaringan yang advanced, memiliki visibilitas terhadap jaringan virtual, memberikan perlindungan yang application-centric dari ancaman pada jaringan dan kemampuan menangani operasi jaringan secara otomatisasi.

Terintegrasi sepenuhnya dalam Nutanix Enterprise Cloud OS dan Nutanix AHV virtualization, Flow memungkinkan organisasi melakukan deployment jaringan virtual yang software-defined tanpa kompleksitas dalam hal pemasangan dan tambahan produk untuk manajemen yang diperlukan.



HPE ARUBA
Aruba IntroSpect

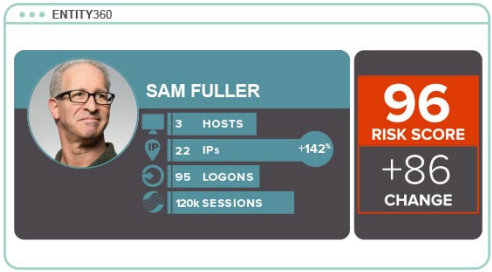
Solusi untuk sektor industri : Semua sektor industri.

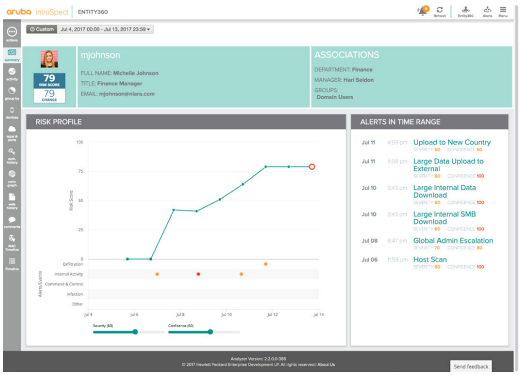
Aruba IntroSpect adalah produk keamanan untuk solusi User and Entity Behavior Analytics (UEBA) dan solusi Network Traffic Analysis (NTA), yang dirancang untuk menganalisa perilaku pengguna dan entitas dalam jaringan enterprise serta menganalisa jaringan lalulintas data yang handal.

Aruba IntroSpect, memiliki kemampuan untuk mendeteksi serangan dengan memantau adanya perubahan hal-hal kecil dalam perilaku dan kebiasaan dari pengguna serta entitas yang ada dalam jaringan.

Aruba IntroSpect mengintegrasikan advanced AI-based machine learning (ML), dengan tampilan visualisasi yang pinpoint sehingga memberikan wawasan forensik, sehingga serangan seperti malicious dari negligent users, sistem dan perangkat sudah dapat diketahui dan segera diatasi.

Entity360 mewakili aktivitas yang relevan dengan keamanan suatu entitas terkait sumber data, perangkat yang digunakan, atau jenis aktivitas. Hal ini mencakup skor risiko (0 hingga 100) serta profil keamanan penuh. Setiap entitas akan memiliki risk score yang berdasarkan kalkulasi machine learning yang akan menjelaskan faktor-faktor kunci.



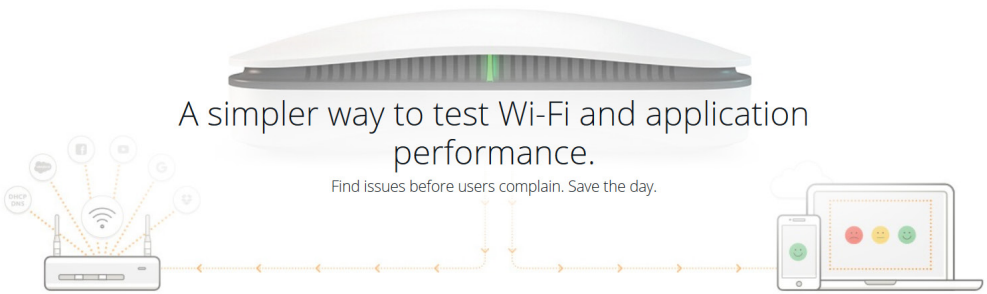


HPE ARUBA
Aruba User Experience Insight

Solusi untuk sektor industri : Semua sektor industri.

Insight adalah sensor diagnosa terhadap kinerja jaringan WiFi dari HPE Aruba yang berbasiskan cloud dengan web-based administrative dashboard yang dapat diakses dari mana saja. Sensor Insight ini dapat ditempatkan dimana saja dan ideal untuk semua enterprise terkait kinerja jaringan, aplikasi dan konektivitas pengguna. Bersama perangkat pengguna dan IoT memantau kinerja jaringan dan konektivitas seperti DHCP, DNS, authentication, captive portal response, cloud dan internal application.

aruba
a Hewlett Packard Enterprise company



Kunjungan CEO dan Vice President DRIVELOCK ke ACS Group

Saat ini, diera Industry 4.0 (era Digital), aspek keamanan siber menjadi sangat penting dan harus diperhatikan. Kelancaran bisnis proses, layanan publik, sistim informasi digital, sangat ditentukan seberapa kuat dan tahan suatu jaringan digital dalam mengatasi serangan kejahatan siber yang terus berlangsung dan terjadi setiap saat.

DriveLock dengan 'Zero-Trust Platform' nya (anti Malware, data loss prevention) bisa menjadi suatu pilihan solusi tepat guna dalam pengamanan tingkat tinggi pada End-Point (end-point protection). Kami PT. Autojaya Idetech, telah ditunjuk sebagai Tier-One-Partner DriveLock di Indonesia dan didukung penuh oleh Manajemen pusat DriveLock Jerman. Hal ini ditandai dengan hadirnya Anton Kreuzer (CEO DriveLock) dan Martin Mangold (VP Cloud Operations DriveLock) ke kantor pusat PT. Autojaya Idetech di Jakarta pada tanggal 3 Desember 2019.

Extreme Networks Bootcamp

Blue Power Technology sebagai value-added distributor Extreme Networks - menyelenggarakan 'EXTREME NETWORKS BOOTCAMP', training singkat selama 2 hari bertempat di daerah Bogor-Jawa Barat. Para peserta termasuk didalamnya beberapa sales dan engineer ACS Group, mereka diberikan pengetahuan presales mengenai produk extreme networks dan berbagai kelebihan yang dimiliki serta solusi-solusi barunya dengan menggunakan berbagai konvergensi jaringan, manajemen, dan fungsi keamanan dalam switching, routing, wireless, manajemen jaringan, dan solusi Kebijakan Extreme Networks. Peserta diharapkan memahami dan menerapkan fungsionalitas yang ada agar dapat memberikan support yang lebih baik kepada customer pengguna extreme networks.

Training DriveLock

Seluruh enginner ACS Group baik pusat maupun cabang mendapatkan training pre sales DriveLock, dimana DriveLock merupakan solusi keamanan endpoint yang mudah dan efektif, memiliki fitur-fitur seperti Encryption, Security Awareness, Drive & Device Control, Application Control dan Analytics & Forensic. Kegiatan training disampaikan oleh Michael Ooi - Senior Pre-Sales Engineer APC DriveLock mengambil tempat di Gedung ACS Group - Jakarta

Atmosphere 2019 APAC

ACS beserta dengan customer Hospitality turut menghadiri acara tahunan yang dipersembahkan oleh HPE Aruba yang dihadiri oleh 1200an membership HPE Aruba, mulai dari Team Aruba, Distributor, Partner hingga End User se-Asia Pacific.

Acara tersebut dibuka oleh Keerti Melkote, President and Founder of Aruba dan Partha Narashiman selaku Chief Technology Officer of Aruba dan team yang memberikan pembahasan mengenai teknologi Wi-fi 6 (802.11ax) dan bagaimana developments dalam wireless dan wired infrastruktur software, network security, location services, dan network analytics & assurance. Hal tersebut juga dikemas berupa agenda yang disajikan dalam beberapa kelas yang bisa diikuti oleh setiap peserta dan diisi oleh pembicara-pembicara dari Aruba Team untuk memberikan informasi lebih detail dan lebih dekat kepada setiap pengunjung yang hadir guna meningkatkan skill networking dalam mengotomatisasi dan menyederhanakan network operations dan hal lainnya terkait dengan product Aruba.

Di Playground, Aruba menyajikan banyak fitur-fitur dalam sebuah spot-spot yang menarik, dimana pengunjung bisa melihat setiap teknologi yang diberikan oleh Aruba dan dapat bertanya langsung kepada Aruba Team di booth tersebut.

24-26 September 2019 - ICC Convention Center, Sydney - Australia

RAKER ACS Group 2019

2020 ACS Corporate Direction & Strategy

Pada tanggal 7 November 2019 ACS Group kembali mengadakan acara rapat kerja tahunan. Raker ini diikuti baik staff Jakarta maupun cabang-cabang dan mengambil tempat di Best Western Plus Kemayoran Hotel - Jakarta.

Acara Rapat Kerja ACS Group ini dibuka oleh Stefan Looho selaku President Director, yang dilanjutkan oleh Indra Tjahjadi - Managing Director yang memaparkan tentang “2020 ACS Corporate Direction & Strategy” yang bertujuan memandu seluruh jajaran agar kegiatan perusahaan sesuai dengan arahan, dan strategi yang disampaikan dapat mencapai target yang telah disepakati bersama.

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

BEING CERTIFIED MEANS WE ARE QUALIFIED TO RUN HIGHER QUALITY JOB FOR YOU AS OUR VALUED CUSTOMER.

Professional Level :

- Aruba Certified Edge Professional (ACEP)
- Aruba Certified Mobility Professional (ACMP)
- Aruba Certified Design Professional (ACDP)
- Aruba Certified ClearPass Professional (ACCP)
- Aruba Certified Switching Professional (ACSP)

Associate Level :

- Aruba Certified Mobility Associate (ACMA)
- Aruba Certified Switching Associate (ACSA)

- Cambium Networks ePMP Certified
- Cisco Certified CCNA
- CWNA Certified
- Extreme Network Certified
- Fortinet NSE Certified
- Hikvision HCSA Certified
- Honeywell Certified
- Microsoft Certified Professional (MCP)
- NCP Nutanix Certified Professional
- Nutanix Certified Systems Engineer: Level 1
- NCSR Nutanix Certified Sales Representative
- Samsung Knox Certified
- Zebra Technologies Certified
- Etc.

SUBSCRIBE

ACS Group Youtube Channel

PT Autojaya Idetech & PT Solusi Periferal (ACS Group)

Things that will you discover.

- Case Study
- Product Highlight
- Unboxing & Tutorial

... etc.

Scan this QRcode

Tips Aman Ketika Menggunakan Wi-Fi Publik

Ketahui resiko ketika kita menggunakan jaringan Wi-Fi *public*, apalagi yang gratis. Tips keamanan kali ini akan membantu melindungi perangkat Anda, serta identitas dan data pribadi Anda dari penjahat dunia maya. Wi-Fi publik tersedia dimana-mana sekarang ini, baik di airport, restaurant, café, hotel dan area publik lainnya. Namun jaringan Wi-Fi ini sangat rentan keamanannya, publik dapat dengan mudah dicegat oleh penjahat *cyber*, atau dikenal dengan serangan *man-in-the middle.*

Bahaya paling umum adalah jaringan Wi-Fi publik palsu atau hotspot palsu yang memang sengaja dibuat sang peretas atau *hacker* dengan memiliki nama yang mirip dengan jaringan hotspot yang sah dan resmi. Setelah Anda terhubung ke jaringan hotspot palsu ini, semua yang Anda lakukan selama online di hotspot palsu tersebut dapat dipantau oleh penjahat *cyber* yang

memindai aktivitas Anda untuk mendapatkan informasi login perbankan dan media sosial.

Koneksi Wi-Fi publik juga dapat digunakan untuk mendistribusikan malware seperti *virus*, *worm*, *trojan horse* hingga *ransomware*. Penjahat dunia maya dapat dengan mudah menanam *virus* dan perangkat lunak berbahaya, sehingga menyebabkan kerusakan serius pada komputer Anda dan membahayakan informasi pribadi Anda.

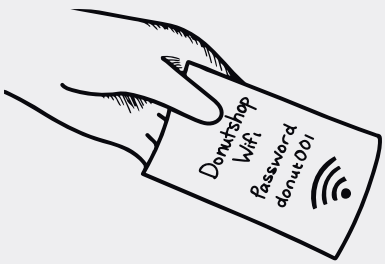
Berikut tips untuk tetap aman ketika menggunakan Wi-Fi publik:

1) Verifikasi koneksi Anda

Mintalah informasi mengenai nama jaringan, *username* dan *password* pada petugas informasi atau *receptionist* sebelum terhubung dengan Wi-Fi *public* agar Anda tidak tersesat ke *hotspot* palsu. Aktifkan *firewall* dan *antivirus* perangkat Anda sebelum terhubung dengan Wi-Fi publik. *Firewall* adalah sistem keamanan jaringan yang memonitor lalu lintas jaringan yang masuk dan keluar. *AntiVirus* untuk mencegah kemungkinan serangan malware seperti *virus* dan lain-lain.

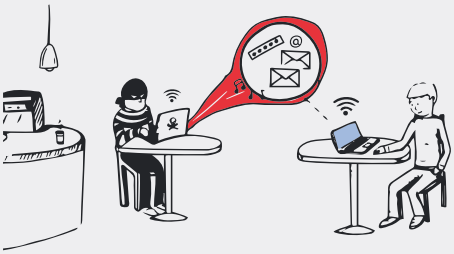
2) Hindari akses ke data yang *sensitive*

Hindari akses perbankan *online*, akses *email*, dan akses yang terkait dengan data yang *sensitive* jika tidak mendesak ketika terhubung internet dengan menggunakan Wi-Fi publik. Pencurian informasi perbankan telah menjadi salah satu jenis kegiatan kriminal yang paling umum di Internet. Selain mencuri kode akses untuk rekening bank pribadi dan rekening bank perusahaan, penjahat *cyber* juga mencuri jumlah kartu kredit dan jenis kartu pembayaran lainnya.



3) Non-aktifkan fitur *file sharing*

Saat tersambung ke Wi-Fi *public* sebaiknya matikan saja fitur sharing jika sedang tidak digunakan karena memberikan pintu masuk tambahan bagi *hacker*. Pastikan file dan folder Anda yang memiliki informasi kritis dan berharga seperti aktivitas *project*, rancangan yang telah dibuat dan data sensitive lainnya telah di-enkripsi. Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga.

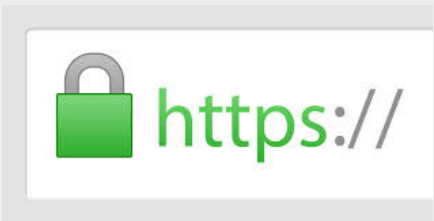


4) Gunakan koneksi VPN

Dengan *Virtual Private Network* atau VPN maka akan menyamarkan identitas pengguna karena data akan di-enkripsi dan mengalihkan transaksi data ke *server* yang aman. Penggunaan VPN adalah salah satu cara yang paling praktis dan efektif untuk mengamankan perangkat saat tersambung ke Wi-Fi *public*.

5) Perhatikan Protokol HTTPS

Pastikan bahwa halaman *web* yang dikunjungi harus terenkripsi dengan protokol https melihat pada *address* bar URL *browser* atau melihat ada tanda gembok keamanan atau tidak pada address bar URL-nya. Situs dengan protokol https menunjukkan bahwa situs web atau halaman web tersebut memiliki beberapa sertifikat digital yang valid bahkan sampai ke titik enkripsi SSL / TLS yang akan mengurangi resiko serangan *Man-in-the-Middle Attack* (MITM) terjadi.

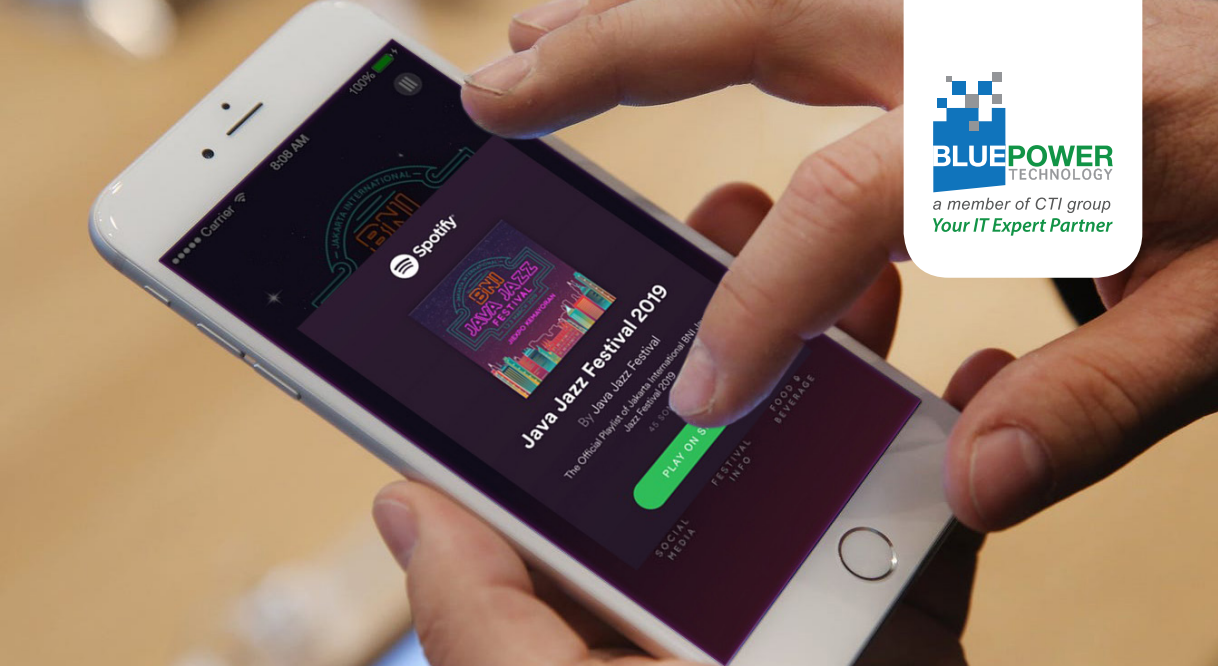


6) Disconnect Wi-Fi *public* setelah selesai

Setelah selesai akses internet dan penggunaan yang seperlunya, segera hentikan koneksi atau *disconnect* perangkat Anda dengan jaringan Wi-Fi *public*. Hal ini bertujuan mengurangi potensi resiko jika Anda terus terhubung dengan jaringan Wi-Fi *public*. Memahami risiko Wi-Fi *public* akan memastikan data penting Anda tidak jatuh ke tangan yang jahat.

Hubungi team *expert* ACS Group untuk pemasangan Wi-Fi *public* jika Anda ingin menyediakan fasilitas *hotspot* di area publik bagi pelanggan dan pengunjung Anda agar para pengguna tetap terlindungi dan mendapatkan koneksi internet yang aman dan handal.

*/ Penulis : Irvan Kurniawan(irvan@acsgroup.co.id)



BLUEPOWER TECHNOLOGY
a member of CTI group
Your IT Expert Partner

Blue Power Technology Kembali Dipercaya Tingkatkan Jaringan dengan Extreme Networks di Java Jazz Festival 2019

Untuk kedua kalinya, Blue Power Technology (BPT) dengan produk andalannya, Extreme Networks, kembali dipercaya pada acara Java Jazz Festival (JJF) yang diselenggarakan pada 1-3 Maret 2019 lalu di JIExpo Kemayoran, Jakarta sebagai penyedia jaringan untuk *Wireless Access Point* mereka. Sebanyak 15 unit WiNG AP8533 yang terpasang berhasil mengakomodasi dan memperkuat jaringan beberapa critical area pada JJF 2019, yaitu area registrasi, *ticket box*, *stan merchandise*, dan area khusus *performer*.

Pada tahun ini, BPT menghadirkan **AP8533(802.11ac)** karena produk ini memiliki fitur *Triple Sensor Technology* dan *Bluetooth Low Energy* (BLE) yang dapat membantu tim pemasaran JJF untuk membagikan dan meng-update informasi penting seputar acara ke pengguna aplikasi JJF secara *real-time*. Fitur ini juga mampu memberikan analisis mengenai informasi pengunjung seperti *gender*, media sosial, demografi, jumlah pengunjung pada masing-masing *stage*, dan lain-lain.

JJF merupakan salah satu festival musik jazz terbesar di Asia Tenggara. Memasuki tahun ke 15-nya, JJF 2019 berhasil mendatangkan lebih dari 100.000 pengunjung. Dengan jumlah pengunjung yang sangat banyak, JJF harus memastikan kinerja dan keamanan jaringan pada area-area penting mereka terjamin dengan mempercayakan BPT sebagai *value-added* distributor dalam menerapkan dan mengintegrasi solusi dari Extreme Networks.

Extreme™
Customer-Driven Networking

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

CORE BUSSINESS SOLUTIONS : 4 PILLARS

Automatic Identification & Data Capture (AIDC) — 1

- Label (Barcode) Printer & Supplies
- Card Printer & Supplies
- RFID Printer & Supplies (RFID Tag)
- Barcode Scanners
- RFID Reader
- Enterprise Mobile Computers
- Enterprise Tablet

IT Infrastructure — 2

- Data Center Solutions
- Hyper Converge Infrastructures
- Enterprise IT Networks Wired & Wireless
- Cyber Security Solutions

Enterprise Security System — 3

- Access Control - Single ID Management
- Alarm System
- IP CCTV

Enterprise Business Solution — 4

- ABB Enterprise Business Solutions
- Roambee - IOT Real-time Shipment Tracking for Supply Chain
- AMTS - Asset Management and Tracking System
- LTS - Laundry Tracking System
- GAS-V - Gate Access System - Vehicle
- ABS - Agriculture Plantation and Mill Management

BUSINESS PARTNERS

ABB · aruba a Hewlett Packard Enterprise company · BarTender by Seagull Scientific · brother at your side · Cambium Networks · DriveLock · Extreme Connect Beyond the Network · FORTINET · Hewlett Packard Enterprise · HID · HIKVISION · Honeywell · ivanti · JANZ · NUTANIX YOUR ENTERPRISE CLOUD · POINT Mobile · roambee · SAMSUNG · Seuic · ZEBRA

Jakarta (HO)
Perkantoran Gunung Sahari Permai #C03-05
Jl. Gunung Sahari Raya No 60-63 Jakarta 10610
Telp : +6221-4208221(H), 4205187(H)
Fax : +6221-4207903, 4207904, 4205853

Cikarang
Cikarang Square Blok E No 62, Jl. Raya Cikarang,
Cibarusah Km 40, Cikarang Barat, Bekasi
Telp : +6221.29612366, 29612367
Fax : +6221.29612368

Semarang
Grand Ngaliyan Square Blok B No.18,
Ngaliyan 50181, Semarang
Telp : +6224.76638092, 76638093
Fax : +6224.76638096

Surabaya
Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo 61254
Telp : +6231-8556277(H); 8556278
Fax : +6231-8556279

Denpasar
Ruko Grand Sudirman Agung Blok B No.29,
Jl. PB Sudirman, Dauh Puri Kelod,
Denpasar Barat, Denpasar - Bali 80114
Telp : +62361-4457859
Fax : +62361-4746526