PERSPEKTIF & WAWASAN GLOBAL

Keamanan siber

BAGIAN 1: Ancaman Siber di Dunia yang Didukung Kecerdasan Buatan

BAGIAN 2: Memastikan Ketahanan Siber

BAGIAN 3: Menetapkan Batas Baru *Zero-trust*

Diterjemahkan oleh IIA Indonesia

IIA Indonesia

The Institute of Internal Auditors

BAGIAN 1

Ancaman Siber di Dunia yang Didukung Kecerdasan Buatan

Tentang para Ahli

Antonio Cacciapuoti, CIA

Antonio Cacciapuoti adalah kepala audit internal di Eurizon Capital S.A. Luxembourg, perusahaan manajemen aset Intesa Sanpaolo Group.

Bradley Niedzielski, CPA

Bradley Niedzielski adalah partner audit dan asurans dan Pemimpin Transformasi Keuangan dan GenAI di Deloitte & Touche LLP, di mana ia melayani perusahaan publik dan swasta di industri jasa keuangan.

Sepanjang tahun lalu, kemajuan kecerdasan buatan (a*rtificial intelligence* atau AI) telah membuat berbagai organisasi berjuang untuk memahami peluang dan ancaman yang ditimbulkan oleh teknologi ini. Sebagai bagian dari upaya tersebut, perusahaan perlu memikirkan bahaya yang dapat ditimbulkan AI pada aspek keamanan, mengingat adanya ketergantungan kepada informasi dan transaksi secara daring. Pelaku kejahatan dengan cepat beralih ke peralatan yang didukung AI untuk meningkatkan kemampuan dalam menerobos pertahanan siber. Tulisan singkat ini mengkaji bagaimana ancaman siber telah berubah di dunia yang digerakkan oleh AI dan bagaimana audit internal membantu perusahaan mengembangkan pendekatan keamanan siber baru sebagai responsnya.

Sebuah Evolusi dalam Kejahatan Siber

Meskipun pertahanan siber yang kuat selalu menjadi perhatian penting, pelaku kejahatan kini menggunakan AI untuk mempertajam dan memperluas kemampuan dalam mengalahkan pertahanan organisasi. “AI bukanlah sebuah serangan baru, melainkan sebuah evolusi,” kata Antonio Cacciapuoti, kepala audit internal di Eurizon Capital S.A. Luxembourg. AI digunakan dengan cara yang lebih canggih daripada serangan siber tradisional dalam hal kecepatan, skala, kompleksitas, dan kemampuan beradaptasi. Selain itu, “seperti virus, AI membangun daya tahan dari waktu ke waktu, sehingga menjadi lebih berbahaya,” katanya.

AI digunakan dalam berbagai serangan, mulai dari serangan dengan fokus tertentu hingga yang berdampak luas. Misalnya, pelaku bisnis saat ini menggunakan dokumen yang dibuat AI untuk e-mail atau laporan, begitupun pelaku kejahatan menggunakan dokumen yang dibuat AI untuk tujuan kriminal, kata Bradley Niedzielski, partner audit dan asurans Deloitte di New York.

Di sisi lain, serangan *phishing* bertujuan untuk menembus keamanan dan mendapatkan akses pada data yang berharga. Meskipun *phishing* bukan hal baru, FBI memperingatkan tentang *phishing* yang didukung oleh AI "yang ditandai oleh kemampuan dalam menyusun pesan yang meyakinkan sesuai pihak penerimanya dengan tata bahasa dan ejaan yang tepat, sehingga meningkatkan kemungkinan berhasilnya penipuan dan pencurian data."

Spear phishing otomatis, misalnya, dipersonalisasi untuk seseorang atau satu kelompok dan ditujukan untuk mencuri informasi sensitif atau akses ke suatu sistem. “AI dapat menganalisis media sosial, pola komunikasi, dan data yang tersedia tentang target, lalu menyusun pesan yang meyakinkan untuk mengelabui penerima agar mengungkapkan informasi sensitif atau mengklik tautan berbahaya,” jelas Cacciapuoti. Pada saat yang sama, ketika dimungkinkan di masa lalu untuk mempercayai suatu video atau telepon berdasarkan pengetahuan atas suara atau ciri khas seseorang, dengan *deepfake* (simulasi video seseorang) dan peretasan suara, yang mereplikasi suara seseorang, dimungkinkan untuk menipu dan memanipulasi target yang spesifik.

Ini bukan satu-satunya ancaman terkait AI. *Malware* yang didukung AI dapat beradaptasi dan mengubah perilakunya berdasarkan lingkungan target, sehingga lebih sulit dideteksi oleh keamanan tradisional, menurut Cacciapuoti. "*Malware* ini dapat dengan mudah lolos dari deteksi dasar dan menggunakan teknik polimorfik untuk mengubah kode dan bahkan menganalisis pertahanan untuk menghindarinya," katanya. Bahkan, dapat memasukkan data yang telah dikontaminasi ke dalam model *machine learning* AI yang digunakan untuk deteksi fraud, sehingga AI membuat prediksi yang tidak akurat dan mengabaikan beberapa indikator fraud.

Dengan menggunakan eksfiltrasi data cerdas, AI dapat menganalisa data curian dan kekayaan intelektual secara *real time* dan memprioritaskan informasi mana yang paling berharga untuk eksfiltrasi. AI kemudian dapat mengenkripsi informasi tersebut dan meminta tebusan untuk melepaskannya, katanya. Serangan yang didukung AI juga dapat membahayakan kredensial yang mengautentikasi pengguna yang valid, memungkinkan mereka berpindah-pindah antar sistem.

Risiko serangan siber yang didukung AI penting karena taruhannya sangat tinggi. Kebocoran atau penyalahgunaan informasi sensitif dapat merusak daya saing organisasi atau menyebabkan terkena sanksi karena gagal mematuhi peraturan privasi data. Setiap pelanggaran dapat menyebabkan pelanggan dan mitra bisnis kehilangan kepercayaan pada

organisasi. Serangan *ransomware* dan *malware* dapat mengganggu operasi dan mematikan sistem yang penting.

Banyak kegunaan yang tidak terbayangkan sebelumnya, tetapi kini sudah mulai digunakan secara nyata. Misalnya, seorang karyawan di perusahaan multinasional di Hong Kong tanpa sengaja membayar $25 juta kepada penipu setelah diyakinkan untuk melakukannya melalui simulasi *deepfake* dari kepala keuangan perusahaan dalam panggilan video, menurut CNN.

Di tempat lain, The Drive melaporkan bahwa seorang eksekutif Ferrari menerima panggilan telepon dari *deepfake* yang mengaku sebagai CEO perusahaan. Upaya itu digagalkan ketika CEO yang mencurigakan itu ditanya sesuatu yang hanya bisa dijawab oleh CEO. Dalam kasus yang dikutip oleh Greylock Partners, seorang mata-mata Korea Utara menggunakan identitas palsu agar direkrut oleh sebuah firma keamanan siber, lalu memasang *malware* pada perangkat perusahaannya.

Pertahanan Terbaik

Untungnya, AI juga dapat membantu organisasi menggagalkan pelaku kejahatan. “Untuk menghentikan AI, Anda harus menggunakan AI,” kata Cacciapuoti. Organisasi perlu mengadopsi keamanan siber yang lebih canggih yang didukung AI untuk mengimbangi ancaman yang terus berkembang. “Jika Anda tidak memiliki pengetahuan tentang teknologi yang digunakan penjahat, bagaimana bisa menghentikan mereka?” tanyanya. Organisasi harus membiasakan diri dengan alat dan strategi yang digunakan penjahat siber dan memahami cara yang dapat membantu meningkatkan keamanan siber.

"The Need for AI-powered Cybersecurity to Tackle AI-driven Attacks," dari ISACA, mengidentifikasi banyak cara teknologi canggih dapat membantu mencegah serangan:

Cara Mencegah Serangan

- Menganalisis kumpulan data secara luas untuk menentukan bagaimana sumber daya organisasi digunakan, menemukan area yang terekspos, inventarisasi aset, dan mengidentifikasi tren lalu lintas jaringan dan aktivitas/perilaku pengguna.
- Mendeteksi anomali, termasuk "login yang tidak biasa, permintaan akses dari lokasi geografis atau alamat IP baru, akses pengguna baru, perubahan izin pada file dan sumber daya lainnya, mengekstrak atau menghapus file dalam jumlah besar, dan peningkatan lalu lintas yang eksponensial."
- Menggunakan AI untuk secara proaktif mengunci, mengeluarkan, atau memblokir tersangka pelaku dan memperingatkan administrator tentang aktivitas mereka.
- Memantau sistem secara terus menerus untuk mengaktifkan respons cepat.
- Menggunakan analisis prediktif untuk mengantisipasi potensi ancaman keamanan dan mengambil langkah-langkah untuk mencegahnya.
- Mendeteksi dan mencegah ancaman *zero-day*, atau kerentanan baru dan tidak terlihat.
- Mengurangi jumlah potensi ancaman palsu atau *false-positive*.
- Mengotomatisasi penilaian keamanan untuk mempercepat respons dan meminimalkan *human error*.
- Penyesuaian untuk beradaptasi dengan perkembangan dan lingkungan baru agar memberikan perlindungan berkelanjutan.

Organisasi dapat memanfaatkan AI untuk menggabungkan, menganalisis, dan mengorelasikan data dari berbagai sumber untuk menciptakan wawasan yang lebih mendalam, kata Cacciapuoti. Mereka juga dapat menggunakan natural language processing (NLP) untuk menganalisis data tekstual yang besar. Misalnya, ketika auditor internal diminta untuk menganalisis kontrak, NLP dapat mengekstrak data tekstual penting untuk dianalisis oleh sistem.

Mengatasi Pertimbangan AI

Karena organisasi tidak akan pernah dapat mengatasi 100% risiko, Niedzielski merekomendasikan untuk memulai dengan menilai ancaman secara strategis di berbagai area bisnis. Itu akan mencakup mengidentifikasi potensi vektor penipuan AI dan mengevaluasi kemungkinan dan dampaknya. Langkah selanjutnya, katanya, menentukan efektivitas pengendalian.

Sebagai bagian dari upaya ini, Niedzielski merekomendasikan GenAI yang baru muncul, seperti penalaran tingkat lanjut dan pengenalan pola, untuk mengenali taktik umum seperti *phishing* dan *deepfake* yang dihasilkan AI. Beberapa perusahaan menggunakan protokol dan teknologi verifikasi apakah panggilan dilakukan dari nomor internal atau eksternal.

"Teknologi canggih ini dapat membantu meminimalkan risiko yang telah dikenali," katanya. Namun, dalam beberapa kasus, seperti membuat keputusan langsung apakah penelepon atau peserta rapat adalah *deepfake*, karyawan mungkin harus mengandalkan naluri atau bersiap mempertanyakan mengapa seorang CEO menelepon dan meminta transfer dana, misalnya. Dalam situasi ini, karyawan didorong memercayai insting mereka dan menelepon kembali orang tersebut ke nomor perusahaan mereka atau, jika penelepon yang dimaksud berada di kantor yang sama, cukup menghampirinya untuk memverifikasi siapa orang itu.

Tim multidisiplin yang terdiri dari profesional berbagai bidang seperti audit internal, manajemen risiko, TI, keamanan siber, dan fungsi relevan lainnya dapat memantau kemajuan dalam AI dan terus memberikan pengkinian untuk manajemen risiko, protokol keamanan, dan sistem deteksi *fraud*. Tim bekerja sama mengidentifikasi dan merespon berbagai upaya, dengan mempertimbangkan berbagai isu seperti kontrol yang paling baik untuk mencegah atau mitigasi kerusakan, kata Niedzielski.

Ia juga menyarankan perusahaan secara berkala berbagi pengalaman dan membahas kerentanan AI. “Bukan hanya upaya yang berhasil, tetapi juga ketika sesuatu berjalan salah dan bagaimana perusahaan belajar darinya,” sarannya. “Berbagi pengetahuan, pelatihan, dan penilaian risiko yang tepat akan memungkinkan untuk meminimalkan risiko *fraud* yang disebabkan oleh AI.”

Di lingkungan ini, pelatihan menjadi prioritas meningkatkan kewaspadaan karyawan tentang potensi aktivitas mencurigakan sekaligus memperkuat tindakan tepat untuk memperbaiki keadaan, kata Niedzielski. Cacciapuoti mencatat bahwa simulasi AI juga dapat digunakan untuk memberikan pelatihan keamanan siber secara langsung dalam situasi dunia nyata. AI dapat menganalisis perilaku karyawan secara individual dalam pelatihan siber dan memberikan wawasan untuk perbaikan.

Kontribusi Audit Internal

Audit internal membantu memastikan upaya organisasi sesuai tantangan AI, kata Cacciapuoti, termasuk memanfaatkan potensi sambil memitigasi risiko. “Audit internal melakukan penilaian risiko komprehensif, mengaudit sistem AI untuk keamanan, etika, dan kepatuhan, serta mendukung inovasi yang aman,” katanya. “Audit internal dapat berpartisipasi dalam membentuk strategi siber yang tangguh dalam mengatasi ancaman AI.”

Selain itu, meskipun audit internal biasanya garis pertahanan, juga berperan sebagai garis ofensif terkait AI, dengan pendekatan dinamis dalam mengelola risiko. "Mengapa menunggu risiko datang jika dapat mengatasinya secara langsung?" tanyanya.

> "AI tidak akan pernah menggantikan auditor internal, tetapi bisa menjadi asisten yang tangguh."
>
> **— Antonio Cacciapuoti, CIA**

Itu berarti menjadi yang terdepan dalam menggunakan teknologi baru sehingga organisasi dapat memaksimalkan peluang sambil memastikan kontrol tata kelola yang tepat dan perbaikan berkelanjutan.

Dalam fungsi audit internal, “AI tidak akan pernah menggantikan auditor internal, tetapi dapat menjadi asisten yang hebat,” menurut Cacciapuoti. Ia mengatakan bahwa audit internal dapat memperoleh manfaat dari penggunaan AI untuk:

- Menganalisis data bervolume besar dan memperluas sampel dalam pengujian agar dekat dengan seluruh populasi.
- Otomasi prosedur pengujian dan memantau kontrol utama, melakukan tugas berulang sehingga auditor internal dapat fokus pada tugas tingkat yang lebih tinggi.
- Menggunakan algoritma AI untuk memantau data secara terus menerus daripada mengandalkan audit berkala, menentukan dan mengatasi aktivitas abnormal lebih cepat.
- Menggunakan analisa prediktif untuk memproyeksikan hasil di masa mendatang dan membuat keputusan dan rekomendasi yang lebih tepat.
- Meringkas kertas kerja dengan cepat agar auditor internal dapat menggunakannya dalam menyusun laporan akhir.

AI memungkinkan pengelolaan temuan yang lebih seragam dan efisien di semua fungsi kontrol. "Di perusahaan yang sangat besar, ada banyak keterlibatan dari berbagai fungsi yang perlu dipertimbangkan," kata Cacciapuoti. AI memungkinkan auditor internal untuk menyatukan data dengan cara yang seragam untuk menghindari duplikasi.

Untuk memitigasi risiko dan memanfaatkan nilainya, Niedzielski merekomendasikan agar auditor internal terus memperbarui pengetahuan mereka tentang kemajuan teknologi. "Ada sesuatu yang baru setiap hari," katanya. Mereka harus fokus pada identifikasi respons proaktif — bukan reaktif — terhadap potensi risiko. Ketika dunia memanfaatkan teknologi baru, auditor internal harus fokus pada tata kelola dan kepatuhan terhadap peraturan baru dan standar etika untuk menjaga integritas organisasi, katanya.

Ancaman Siber yang Didukung AI: Fakta Singkat

- 97% profesional keamanan khawatir organisasi mereka akan mengalami insiden keamanan siber yang dihasilkan AI, karena AI terus menyebabkan kelelahan.
- 75% profesional keamanan harus mengubah strategi keamanan siber mereka pada tahun lalu karena meningkatnya ancaman siber yang didukung AI.
- 73% tim keamanan ingin lebih fokus pada kemampuan yang mengutamakan pencegahan.
- 61% organisasi melihat peningkatan insiden *deepfake* selama setahun terakhir.
- 75% dari serangan ini menyamar sebagai CEO organisasi atau anggota *C-suite* lainnya.

Sumber: G*enAI in Cybersecurity: Friend or Foe? Voice of SECOPS*, Edisi ke-5 2024

"Auditor internal harus menempatkan diri mereka pada posisi pelaku kejahatan," menurut Niedzielski. "Jangan tanya bagaimana pelaku akan menyusup ke organisasi, tanyakan apa yang akan Anda lakukan jika Anda adalah pelaku kejahatan berdasarkan apa yang Anda ketahui tentang organisasi. Pertimbangkan tidak hanya perspektif kuantitatif, tetapi juga kualitatif, tentang organisasi."

Auditor internal tidak boleh mencoba melakukannya sendiri, kata Cacciapuoti, yang merekomendasikan koordinasi dengan semua penyedia asurans dan pemangku kepentingan untuk mencegah dan memitigasi risiko, termasuk yang berada dalam fungsi pengendalian, kepatuhan, manajemen risiko, auditor eksternal, dan regulator. "Kolaborasi antara alat AI dan profesional keamanan siber, di samping kerangka kerja tata kelola yang kuat, sangat penting untuk menavigasi lanskap ini dan menanggapi risiko baru yang muncul," katanya.

BAGIAN 2

Memastikan Ketahanan Siber

Tentang para Ahli

DC Chang, CPA, CDPSE, CISSP, CRISC, CISA

DC Chang adalah direktur audit, Teknologi Digital dan Keamanan Siber, di United Airlines di Dallas, Texas.

Michael Echols, CISSP

Michael Echols adalah CEO Max Cybersecurity LLC di Washington, DC.

Justin Headley, CPA, CISSP, CISA, CRISC

Justin Headley adalah manajer senior di Grup Jasa Advis & Asurans Risiko Warren Averett di Birmingham, Alabama.

Meskipun organisasi berupaya memastikan memiliki perangkat memadai untuk mencegah serangan siber, hampir dapat dipastikan mereka akan mengalami penetrasi atau serangan dalam bentuk apa pun. Mengingat hal itu, bisnis harus berfokus pada kemampuan untuk merespon dan pulih dengan cepat dari serangan siber. Ringkasan ini membahas cara terbaik memahami dan menanamkan ketahanan terhadap serangan dan menjelaskan peran auditor internal dalam memperkuat respon organisasi.

Menyiapkan Panggung untuk Pemulihan

Ketahanan siber yang terbaik bukan sekadar reaksi terhadap situasi yang mengerikan. Ketahanan siber merupakan rangkaian praktik — perencanaan, proses, analisis, pelatihan, layanan penting, dan manajemen — yang memastikan organisasi dapat mempertahankan operasinya, menurut Michael Echols, CEO Max Cybersecurity LLC. Praktik-praktik ini memungkinkan pemulihan atau pemeliharaan fungsi organisasi setelah serangan, tetapi praktik-praktik ini harus diterapkan jauh sebelum masalah terjadi.

Misalnya, Echols bekerja dengan klien firma hukum yang menerima semua rujukan melalui situs webnya. Biasanya, firma ini menerima banyak rujukan setiap hari, tetapi pada satu titik, dua hingga tiga hari berlalu sebelum firma tersebut menyadari bahwa mereka tidak menerima rujukan apa pun dan akhirnya menyadari bahwa situs webnya telah diretas. "Firma tersebut seharusnya sudah memiliki proses untuk pemantauan berkelanjutan dan untuk beberapa jenis pemberitahuan" tentang penurunan rujukan web yang tidak biasa, karena rujukan web merupakan sumber bisnis utama firma tersebut (fungsi yang sangat penting), katanya.

Masalah yang perlu diidentifikasi — seperti penurunan *web traffic* — akan berbeda untuk setiap bisnis dan kemungkinan akan ada lebih dari satu. Dalam banyak kasus, organisasi ingin bersiap menghadapi insiden yang akan memengaruhi pasokan listrik mereka, misalnya, dengan langkah-langkah untuk menyebarkan generator yang terpisah dari bisnis utama, sehingga mereka tidak terpengaruh oleh serangan tersebut, kata Echols.

> Ketahanan siber adalah "kemampuan untuk mengantisipasi, bertahan, memulihkan, dan beradaptasi dengan kondisi, tekanan, serangan, atau gangguan pada sistem yang menggunakan atau didukung oleh sumber daya siber. Ketahanan siber dimaksudkan untuk memungkinkan tercapainya misi atau tujuan bisnis yang bergantung pada sumber daya siber dalam lingkungan siber yang penuh tantangan."
>
> **— U.S. National Institute of Standards and Technology**

Mempersiapkan apa yang akan terjadi mengharuskan penempatan lingkungan keamanan siber saat ini, menurut DC Chang, direktur audit, Teknologi Digital dan Keamanan Siber, di United Airlines. Dua puluh tahun yang lalu, organisasi memiliki pusat data mereka sendiri, dan keamanan siber, sampai batas tertentu, adalah masalah mengunci server di balik pintu dan jendela fisik. Saat ini, data disimpan di lingkungan virtual yang dapat rentan terhadap aktor jahat di seluruh dunia.

"Ada jutaan jendela dan pintu yang perlu kami lacak sekarang karena kami digital, bahkan ditambah dan dihapus setiap hari," kata Chang. Organisasi perlu menyadari kecepatan dan ruang lingkup akselerasi digital untuk mengembangkan ketahanan yang mereka butuhkan dalam krisis.

Tata Kelola dan Budaya

Tata kelola memiliki peran penting dalam membangun ketahanan siber, menurut Justin Headley, manajer senior di Grup Jasa Advis dan Asurans Risiko Warren Averett. "Kami terus-menerus mendengar bahwa karyawan adalah titik lemah karena mereka menggunakan kata sandi yang lemah atau mengklik tautan yang mencurigakan," katanya. "Namun, jika para pemimpin tidak terlibat, Anda tidak dapat mengharapkan karyawan untuk melakukan tanggung jawab mereka."

Dalam banyak hal, keamanan siber tidak sepenuhnya merupakan masalah teknologi, tetapi juga masalah budaya. "Jika Anda mengubah pikiran 90% orang di organisasi dan satu orang membuka tautan di email, hal tersebut bisa menghancurkan perusahaan," kata Echols. Budaya sadar keamanan siber memperjelas ekspektasi organisasi dan meyakinkan konsumen dan mitra bisnis. "Bank adalah salah satu kelompok pertama yang menjadi *cyber resilient*," katanya, karena mereka mengandalkan kepercayaan pemangku kepentingan mereka.

Headley merekomendasikan para pemimpin untuk menumbuhkan budaya keamanan siber yang melampaui pendekatan standar seperti email triwulanan yang berisi tip keselamatan siber atau pelatihan keamanan tahunan yang belum sempurna. Langkah-langkah yang diambil organisasinya termasuk mengirimkan email *phishing* palsu sendiri kepada karyawan, kemudian memberikan pelatihan kepada mereka yang mengklik tautan mencurigakan yang disematkan. "Anda harus menunjukkan bagaimana tata kelola siber bekerja dalam tindakan, bukan hanya secara teori," katanya.

Para pimpinan juga dapat memberikan langkah-langkah spesifik untuk diambil saat berada dalam serangan. "Sebuah organisasi dapat menghentikan serangan dan pulih jika ada kebijakan dan prosedur yang praktis dan dapat diulang untuk diikuti jika terjadi serangan," menurut Headley. Jika para pimpinan terlibat ketika langkah-langkah ini diuji dan mengambil bagian dalam menyelesaikan masalah, mereka menunjukkan komitmen mereka terhadap upaya tersebut, yang dapat memainkan peran besar dalam menyukseskan strategi keamanan siber mereka.

- 68% pelanggaran melibatkan elemen manusia yang tidak berbahaya, seperti seseorang yang terjerumus dalam serangan rekayasa sosial atau membuat kesalahan.
- Waktu rata-rata bagi pengguna untuk terbawa oleh surat elektronik *phishing* kurang dari 60 detik.
- 15% pelanggaran melibatkan pihak ketiga atau pemasuk, termasuk rantai pasokan perangkat lunak, mitra infrastruktur *hosting*, atau kustodian data.

Sumber: Verizon Business 2024 Data Breach Investigation Report

Dampak Regulasi

Dalam aturan final tentang Manajemen Risiko, Strategi, Tata Kelola, dan Pengungkapan Insiden Keamanan Siber, Komisi Sekuritas dan Bursa AS meningkatkan ekspektasi bagi organisasi dengan mensyaratkan perusahaan publik untuk mengungkapkan insiden keamanan siber yang material dan membuat pengungkapan berkala tentang bagaimana mereka menilai, mengidentifikasi, dan mengelola risiko siber. Aturan itu "menyoroti hal penting yang harus dipertimbangkan oleh setiap entitas di planet ini," kata Chang.

Di antara persyaratannya, aturan tersebut memaksa organisasi untuk memastikan praktik siber mereka beroperasi, kata Headley. Dia mencatat bahwa fungsi TI sering beroperasi secara terpisah-pisah (silo), yang dipahami secara dengan tersirat oleh para pemimpin tanpa sepenuhnya memahami cara kerjanya. "Hal itu harus diubah," katanya. Harus ada pemahaman di seluruh organisasi tentang cara memperlakukan data internal dan pelanggan serta mengatasi masalah siber.

Seperti halnya banyak peraturan, "semuanya akan bermuara pada transparansi," kata Echols. "Ketika ada pelanggaran material, perusahaan harus memiliki proses yang jelas tentang bagaimana ia bereaksi terhadap pelanggaran itu."

Menambahkan AI ke dalam Perpaduan

Kecerdasan artifisial (AI) dapat menjadi alat yang sangat berharga dalam meningkatkan pencegahan masalah siber dan ketahanan setelah serangan. Teknologi seperti *firewall* generasi berikutnya dan sistem *point protection* membuatnya lebih mudah untuk memilah lalu lintas data dan menemukan anomali yang harus diselidiki, kata Headley. "Penggunaan AI telah menjadi pengubah permainan dalam beberapa tahun terakhir, dan akan terus membantu perusahaan menjadi lebih baik dalam mendeteksi dan merespon serangan."

KA juga dapat digunakan sebagai senjata melawan organisasi. "Jika Anda memiliki kerentanan yang telah diabaikan, AI akan membantu peretas menemukannya," kata Echols.

Di antara pertimbangan lainnya, organisasi harus menyeimbangkan antara dorongan untuk meningkatkan efisiensi secara lebih besar yang diperoleh melalui alat baru dan kebutuhan untuk melindungi keamanan dan privasi, menurut Headley. Teknologi baru membantu organisasi menghilangkan tugas-tugas berulang, yang sering kali melibatkan pemberian informasi sensitif dalam program. Pada saat yang sama, "kami terus melihat serangan yang menargetkan teknologi ini karena pelaku kejahatan tahu bahwa orang tidak sepenuhnya memahami teknologi," yang dapat membuat data sensitif yang terkandung dalam program menjadi sangat rentan.

Dalam membangun ketahanan, organisasi harus melatih karyawan mereka dalam bidang teknologi yang berkembang dan memastikan penggunaan teknologi sesuai dengan selera risiko organisasi. "Sebuah perusahaan dapat memiliki teknologi dan keahlian terbaik, tetapi pengguna mungkin masih tanpa sadar atau terkadang dengan sengaja membocorkan data melalui pintu depan menggunakan alat GenAI," kata Headley.

Organisasi juga harus berhati-hati untuk tidak mengabaikan pendekatan serangan siber tradisional. Banyak masalah dunia maya disebabkan oleh masalah yang bukan baru, seperti kesalahan konfigurasi atau kegagalan untuk mengikuti praktik yang sudah mapan, kata Echols. Banyak pelanggaran terkait dengan kerentanan yang diketahui yang tidak pernah diperbaiki atau tambalan yang belum diinstal, katanya. Akibatnya, mengedukasi pengguna akhir tentang ancaman baru dan yang sudah ada sangat penting. "Auditor harus memeriksa secara lebih mendalam dan mengajukan pertanyaan yang tepat kepada klien untuk menggali kerentanan tersembunyi yang muncul olehsikap apatis," katanya.

"Pemangku kepentingan, terutama dewan dan manajemen senior, mengandalkan jasa asurans yang independen, objektif, dan kompeten untuk memverifikasi apakah respon insiden siber dan kontrol pemulihan dirancang dengan baik dan diterapkan secara efektif dan efisien. Fungsi audit internal menambah nilai bagi organisasi ketika menyediakan jasa tersebut sesuai dengan Standar dan dengan referensi ke kerangka kerja kontrol yang diterima secara luas, terutama yang secara tegas digunakan oleh fungsi teknologi dan keamanan informasi organisasi ."

Sumber: Panduan Audit Teknologi Global: Mengaudit Respons dan Pemulihan Insiden Siber, Edisi ke-2, Panduan Praktik Global, Institut Auditor Internal, 2024

Bagaimana Audit Internal Dapat Membantu Meningkatkan Ketahanan

Dalam lingkungan ini, audit internal harus dipersiapkan untuk membingkai hasil audit mereka untuk meningkatkan ketahanan dan mengidentifikasi kerentanan dengan cara yang membantu klien memahami konsekuensi potensial dari keamanan siber yang lemah, kata Echols. Sementara klien mungkin berasumsi yang terburuk tidak akan pernah terjadi pada mereka, auditor internal harus dapat menangguhkan ketidakpercayaan, yang akan lebih memungkinkan mereka untuk membayangkan hal yang tak terbayangkan. Misalnya, Echols memiliki klien yang memiliki praktik terbaik yang melarang penggunaan alamat email perusahaan di akun media sosial, tetapi itu bukan kebijakan resmi. Kesalahan pendekatan itu menjadi jelas ketika MGM mengalami pelanggaran data yang signifikan akhir tahun lalu. Investigasi pelanggaran tersebut dilaporkan mengungkapkan bahwa seorang karyawan menggunakan email kerja mereka di platform media sosial. Peretas menemukan informasi karyawan di LinkedIn dan menyamar sebagai karyawan untuk melakukan panggilan ke *help desk* TI MGM sehingga memperoleh kredensial untuk mengakses dan menginfeksi sistem MGM. "Praktik terbaik berasal dari pengalaman banyak orang dan harus dibuat kebijakan, jika memungkinkan," kata Echols.

Auditor internal juga harus memahami bahwa aspek kepatuhan audit hanyalah langkah awal dalam membantu membangun ketahanan siber. "Kepatuhan bukanlah keamanan," kata Echols. Auditor internal harus fokus untuk menerjemahkan temuan mereka ke dalam wawasan yang lebih besar yang dapat digunakan tim klien untuk meningkatkan keamanan dan mengajukan pertanyaan yang mungkin belum dapat dijawab oleh tim.

"Anda harus dapat menginstruksikan klien bahwa dengan tidak mencari dan menemukan jawaban atas pertanyaan ini sesungguhnya benar-benar menciptakan kerentanan," menurut Echols.

Di antara audit yang dilakukan, audit internal harus menjaga jalur komunikasi tetap terbuka dengan menjadwalkan waktu untuk memeriksa dan mempelajari tantangan tim. "Ketika auditor internal dapat memposisikan diri mereka sebagai penasihat terpercaya, itu benar-benar mengubah permainan," kata Headley.

Transparansi sangat penting. Auditor internal harus jelas dalam menentukan ruang lingkup dan prosedur pengujian yang direncanakan, serta masalah apa yang muncul. "Pastikan untuk berkomunikasi lebih awal dan sering," katanya, "terutama ketika melibatkan risiko TI." Dia menyarankan agar auditor internal menghindari penilaian segera yang terburu-buru, tetapi sebaliknya melakukan percakapan terbuka tentang proses pemikiran tim klien dan mendorong kolaborasi dengan tim klien.

Headley mencatat bahwa tim TI sering terjebak dalam memenuhi tuntutan berbagai lini bisnis, bertanggung jawab atas segala hal mulai dari menjaga aplikasi tetap aktif dan berjalan, hingga menangani gangguan perangkat keras sehari-hari. Akibatnya, keamanan siber mungkin tidak selalu menjadi prioritas utama. Auditor internal dapat mempromosikan kesadaran akan tantangan ini dan mengedukasi tim tentang peluang untuk mengatasinya, sehingga memastikan audit adalah latihan nilai tambah yang sebenarnya.

"Auditor internal dapat menjadi mitra dalam membantu memperkuat ketahanan perusahaan," kata Headley. Di antara langkah-langkah lainnya, mereka dapat membantu memuluskan pemutusan hubungan antara pemimpin perusahaan dan tim TI, yang seringkali tidak berbicara dalam bahasa yang sama. Karena auditor internal memahami risiko bisnis dan risiko TI, mereka dapat membantu menjembatani kesenjangan itu

Auditor internal juga dapat membentuk pemahaman tentang risiko siber dan pemecahan masalah terkait dengan cara yang berangkat dari praktik masa lalu, kata Chang. Saat organisasi menjauh dari perencanaan kelangsungan bisnis atau pemulihan bencana bisnis tradisional, auditor internal dapat membantu mereka mengadopsi pendekatan yang lebih beragam dan bernuansa. Mereka dapat meningkatkan upaya itu dengan mengambil peran sebagai pendongeng yang memproses informasi dan titik data yang terputus, serta menyatukannya menjadi narasi menarik yang mendorong pengambilan keputusan yang lebih baik.

Menyeimbangkan Keadaan

Pada akhirnya, ketahanan berarti menerima serangan yang tak terelakkan dan berasumsi bahwa dinding luar organisasi adalah tidak dapat ditembus, catat Echols. Sebagai bagian dari upaya itu, organisasi harus mengakui bahwa mereka berada dalam pertarungan yang tidak adil. Sementara organisasi berusaha untuk memblokir 100% serangan yang mereka hadapi, peretas hanya perlu membuka satu pintu untuk mendatangkan malapetaka, kata Chang. "Jauh lebih sulit untuk menjadi pembela daripada pelaku," katanya. Audit internal dapat memberikan wawasan dan informasi yang dibutuhkan perusahaan mereka untuk meningkatkan peluang keberhasilan keamanan siber mereka.

Menurut survei kepada pembuat keputusan TI dan operasi keamanan:

Hanya 2% responden yang mengatakan mereka dapat memulihkan data mereka dan memulihkan proses bisnis dalam waktu 24 jam setelah serangan siber.

69% mengatakan organisasi mereka telah membayar uang tebusan dalam setahun terakhir, meskipun 77% mengatakan mereka memiliki kebijakan atau protokol yang ditentukan untuk tidak membayar uang tebusan.

42% mengatakan organisasi mereka dapat mengidentifikasi data sensitif dan mematuhi undang-undang dan peraturan privasi data yang berlaku. Yang lain tidak memiliki kemampuan TI dan keamanan yang memadai untuk melakukan keduanya.

Sumber: Laporan Ketahanan Siber Global Cohesity 2024

BAGIAN 3

Menetapkan Batas Baru *Zero-trust*

Tentang para Ahli

Adam Kohnke

Adam Kohnke, yang berbasis di Madison, Wisconsin, adalah manajer keamanan informasi dari perusahaan manufaktur kimia Charter Next Generation.

Julio Tirado

Julio Tirado adalah wakil presiden eksekutif, direktur Audit Internal dan Kepatuhan, di SpiritBank, yang berbasis di Tulsa, Oklahoma.

Menjaga keamanan jaringan seharusnya merupakan persyaratan dasar bagi setiap organisasi untuk memiliki proses dan kontrolnya. Namun, seiring kemajuan teknologi dan jaringan yang telah tumbuh lebih besar dan hampir tidak terduga kompleksitasnya, standar yang mencerminkan suatu jaringan aman telah berubah. Salah satu perubahan terpenting terletak pada transisi dari model keamanan yang berpusat pada lokasi (*location-centric*) ke model yang lebih berpusat pada data (*data-centric*). Kami menyebut model ini "*zero trust*".

Apa itu *Zero Trust*?

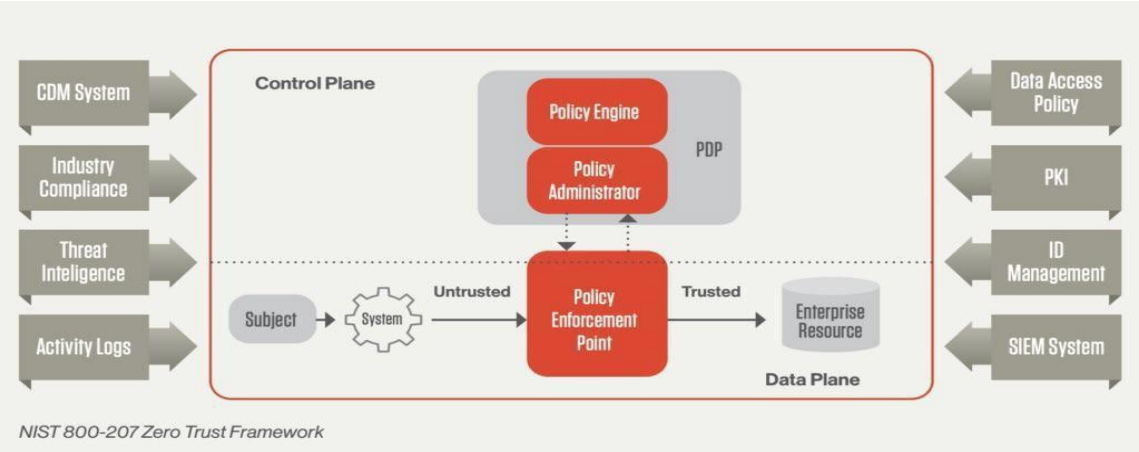
Umumnya, kerangka kerja keamanan *zero-trust* mengharuskan semua pengguna yang beroperasi di dalam jaringan — baik di dalam maupun di luar organisasi itu sendiri — untuk diotentikasi sebelum mengakses aplikasi dan data, dan kemudian terus divalidasi secara teratur. Sesuai dengan namanya, "kepercayaan", atau lebih khusus lagi "percaya tetapi verifikasi", tidak berperan dalam sistem ini dan akses ke apa pun yang berhubungan dengan perusahaan harus terus disesuaikan dan dinilai berdasarkan kebijakan organisasi.

Secara tradisional, model siber dibangun berdasarkan lokasi jaringan, tetapi dalam sistem *zero-trust*, apa yang merupakan "jaringan" kurang didefinisikan secara ketat, karena jaringan organisasi dapat bersifat lokal, berbasis *cloud*, atau hibrida dari keduanya. Setelah pandemi COVID-19, yang mengantarkan era baru kerja jarak jauh, sistem hibrida atau sepenuhnya berbasis *cloud* secara khusus telah menjadi norma, dan kerangka kerja keamanan siber harus berkembang untuk memperhitungkannya.

Ada beberapa kerangka kerja formal *zero-trust*, termasuk:

- Standar 800-207 dari National Institute of Standards and Technology (NIST). Ini adalah kerangka kerja yang diamanatkan untuk digunakan oleh lembaga federal AS sejak 2021 (Lihat Gambar 1).
- Google BeyondCorp.
- Strategi Microsoft Zero Trust.
- Model Kematangan Zero Trust dari Cybersecurity and Infrastructure Security Agency (CISA).

Gambar 1



Sumber: Jaringan Zero Trust | NIST

Meskipun mereka semua memiliki atribut uniknya masing-masing, masing-masing memiliki prinsip dasar yang sama, yaitu:

- Secara terus-menerus memverifikasi akses di semua sumber daya.
- Meminimalkan area dampak atas kejadian pelanggaran eksternal atau internal.
- Penggunaan data perilaku untuk mengumpulkan konteks dari infrastruktur TI.

Meskipun transisi ke sistem semacam itu bisa tampak substansial, penting untuk dicatat bahwa hal itu tidak dimaksudkan untuk menjadi pengganti sistem saat ini. "*Zero trust* tidak berusaha untuk sepenuhnya menggantikan model perlindungan jaringan saat ini atau bahkan perubahan infrastruktur," kata Adam Kohnke, manajer keamanan informasi di perusahaan manufaktur kimia Charter Next Generation, "melainkan sebagai penguatan untuk meningkatkan perlindungan jaringan. Ini dimaksudkan untuk menjadi perluasan karena sistem tradisional seperti *firewall*, *proxy web*, dan mekanisme isolasi batas tidak berfungsi."

Menurut IBM, biaya rata-rata satu pelanggaran data pada tahun 2024 adalah $4,88 juta. Selain itu, siklus hidup rata-rata pelanggaran adalah 292 hari penuh dari identifikasi hingga penahanan. Jelas, perlindungan jaringan tradisional belum cukup dan membutuhkan perhatian yang signifikan.

Peran Audit Internal

Meskipun detailnya dapat bervariasi, auditor internal dapat memiliki berbagai tanggung jawab yang terkait dengan implementasi dan pemeliharaan sistem *zero-trust*. Sebagai ilustrasi, berikut adalah area di mana penilaian audit internal mungkin memiliki nilai paling besar.

Mendefinisikan Permukaan yang Dilindungi

Secara tradisional, sistem keamanan siber memusatkan upayanya untuk menentukan parameter keamanan apa di sekitar jaringan perusahaan. Sistem *firewall* dan VPN dirancang berdasarkan konsep ini, menjaga data sensitif dan rentan informasi sejauh mungkin dari perimeter jaringan. Dalam

sistem *zero-trust*, alih-alih parameter, fokusnya adalah pada pengelompokan data, aplikasi, aset, dan layanan atau *data, applications, assets, and service* (DAAS) yang dikenal secara kolektif sebagai "melindungi permukaan."

Memastikan permukaan ini diidentifikasi dengan tepat harus menjadi inti dari penilaian audit internal yang komprehensif.

Menurut Julio Tirado, wakil presiden eksekutif, direktur Audit Internal dan Kepatuhan di SpiritBank, "Penilaian harus fokus pada pemeriksaan kebijakan klasifikasi data organisasi untuk menentukan apakah sistem dan data diklasifikasikan dengan tepat, dan apakah kebijakan perlindungan yang berlaku untuk masing-masing sesuai dengan tepat."

Layanan yang dilindungi juga tidak hanya terbatas pada data, kata Tirado. Aset fisik yang memiliki peran dalam mengakses data sensitif juga harus memiliki proses dan prosedur untuk memastikannya diinventarisasi dan dinilai secara berkala.

> Penilaian harus fokus pada pemeriksaan kebijakan klasifikasi data organisasi untuk menentukan apakah sistem dan data diklasifikasikan dengan tepat, dan apakah kebijakan perlindungan yang berlaku untuk masing-masing sesuai dengan tepat.
>
> **— Julio Tirado, SpiritBank**

Memverifikasi Peta Alur Transaksi

Setelah ada asurans bahwa permukaan perlindungan diidentifikasi, langkah selanjutnya dalam proses penilaian adalah memastikan bahwa ada pemahaman pemangku kepentingan tentang bagaimana semua sistem DAAS ini berinteraksi satu sama lain. Tim TI harus memiliki diagram dokumentasi terperinci yang didedikasikan untuk memetakan jaringan *port* yang kompleks, garis besar lalu lintas jaringan, dan protokol yang secara kolektif menguraikan bagaimana sistem ini saling mengakses satu sama lain dan ke mana penggunaannya dapat mengarah.

Meskipun di sebagian besar organisasi fungsi audit internal mungkin tidak memiliki pengetahuan atau pengalaman yang cukup untuk memverifikasi keakuratan diagram ini sendiri, Kohnke mengatakan audit internal dapat bekerja dengan pemangku kepentingan atau pihak ketiga tepercaya untuk memverifikasi pengujian validasi telah dilakukan untuk memastikan apa yang digambarkan cukup. "Yang penting," katanya, "adalah bahwa DAAS yang relevan diperhitungkan dalam setiap diagram dan jika ada detail yang cukup ... dan apakah kebijakan keamanan awal yang ditentukan dalam langkah-langkah sebelumnya telah dimodifikasi atau memerlukan pengendalian tambahan."

Memverifikasi Pembuatan dan Peningkatan Berkelanjutan Kebijakan Zero-trust

Kebijakan *zero-trust* harus dirinci untuk setiap permukaan pelindung dan harus menjawab pertanyaan penting seperti:

- Siapa yang harus diizinkan untuk mengakses sistem DAAS perusahaan?
- Aplikasi apa yang akan diizinkan untuk mengakses sistem DAAS perusahaan?
- Kapan akses ke sistem DAAS perusahaan harus terjadi atau sedang terjadi?
- Di mana sistem DAAS perusahaan berada?
- Mengapa sistem DAAS perusahaan perlu diakses?
- Bagaimana seharusnya akses ke sistem DAAS perusahaan diberikan?

Untuk menilai relevansi dan validitas kebijakan *zero-trust* yang dibuat, interaksi berkelanjutan dengan pemangku kepentingan TI sangat penting karena jaringan perusahaan terus berkembang dan berkembang. "*Zero trust* bukanlah tujuan," kata Tirado, "sehingga kebijakan keamanan dan persyaratan perlindungan DAAS harus berkembang seiring berjalannya proses."

Tujuannya, kata Tirado, harus memiliki kebijakan yang terus meningkat yang didedikasikan untuk menangani setiap jenis lalu lintas yang dapat masuk, keluar, dan melintasi jaringan. "Seharusnya tidak ada apa pun dalam jaringan yang sumber atau tujuannya tidak dapat diidentifikasi," katanya. "Auditor internal dalam penilaian mereka perlu menentukan apakah tinjauan dilakukan, apakah mereka dilakukan pada tingkat yang memadai, dan apakah kebijakan yang ada secara akurat membahas apa yang mereka temukan."

Pemantauan Arsitektur Zero-trust

Seperti yang ditunjukkan oleh contoh sebelumnya, pemantauan berkelanjutan sangat penting untuk keberhasilan kerangka kerja *zero-trust*. Tidak seperti sistem tradisional dengan pemantauan akan berfokus pada parameter keamanan, sistem pemantauan sistem *zero-trust* akan berpusat di sekitar pengguna, perangkat, dan layanan. "Pemantauan harus dilakukan pada jaringan Anda untuk mengukur kinerja, mengidentifikasi semua perangkat yang terpasang ke jaringan Anda, dan mendeteksi perangkat nakal dan aktivitas berbahaya," kata Pusat Keamanan Siber Nasional dalam panduan *zero-trust*. Ini terutama berlaku jika Anda menghosting layanan di tempat, tetapi karena telah menjadi lebih umum, manajemen perangkat seluler harus dipertimbangkan dalam ukuran yang sama.

> Pemantauan harus dilakukan di jaringan Anda untuk mengukur kinerja, mengidentifikasi semua perangkat yang terpasang ke jaringan Anda, dan mendeteksi perangkat nakal dan aktivitas berbahaya.
>
> **— Pusat Keamanan Siber Nasional**

"Perusahaan seperti milik saya akan menyebarkan perangkat lunak manajemen perangkat seluler yang akan memberikan ukuran pengendalian untuk perangkat tertentu, selama pengguna menerimanya," kata Tirado. "Perangkat akan memantau aktivitas, membantu membatasi situs berbahaya, membatasi perangkat lunak tertentu yang dapat diinstal pada perangkat, dan memberikan kontrol untuk menyebarkan pembaruan ke sistem tertentu."

Selain itu, pemantauan harus mencakup tidak hanya penggunaan sistem yang sebenarnya, tetapi juga berapa lama mereka digunakan. Seperti yang dinyatakan oleh Pusat Keamanan Siber Nasional, "Perilaku pengguna, seperti jam kerja normal

atau lokasi kerja normal, adalah metrik penting untuk dipantau."

Ada berbagai sistem pemantauan yang tersedia yang dirancang untuk memenuhi kebutuhan spesifik jaringan yang bersangkutan, tetapi umumnya, sistem ini akan mentransfer data yang dikumpulkan ke lokasi pusat di mana data tersebut kemudian dapat dianalisis. Informasi ini, seiring waktu, akan menetapkan "acuan" untuk apa yang merupakan perilaku normal mengenai variabel seperti volume transaksi, komunikasi aset, dan aktivitas pengguna.

Melalui penilaian mereka, auditor internal dapat memastikan bahwa tinjauan rutin terhadap data ini dilakukan — dan bahwa manajemen mengambil kepemilikan yang tepat atas tugas ini — dan bahwa temuan mereka menciptakan acuan yang secara akurat mencerminkan realitas jaringan.

"Bagi auditor internal, banyak hal yang bermuara pada tata kelola," kata Tirado. "Manajemen harus terinformasikan tentang peran yang mereka mainkan dalam mengamankan sistem, karena sistem tidak akan bertahan lama dengan sendirinya. Perubahan kebijakan keamanan ditentukan oleh apa yang ditetapkan oleh acuan sebagai 'normal' dan 'abnormal'. Tinjauan manajemen menetapkan acuan tersebut."

Menetapkan Acuan

Seperti banyak elemen keamanan siber, atau memang manajemen risiko, tidak ada model "satu ukuran yang sesuai untuk semua", dan dengan demikian, bagaimana fungsi audit internal berkontribusi padanya akan sangat bervariasi. "Itu tergantung pada sumber daya," kata Tirado. "Itu tergantung pada ukuran organisasi. Hal tersebut tergantung pada mandat tim audit internal."

Tempat yang baik untuk menetapkan acuan, katanya, adalah memetakan proses pemberian asurans yang tidak berbeda dengan sistem audit lainnya. "Sebagai contoh, pikirkan Sarbanes-Oxley," katanya. "Setiap perusahaan publik harus memetakan pengendalian internal terkait laporan keuangan, mengembangkan matriks ini. Dan sebagai bagian dari pemetaan itu, Anda akan membuat prosedur pengujian melalui periode tertentu — seperti tahun tertentu. Anda akan mengambil pendekatan yang sama dengan *zero trust*, memecah asurans menjadi beberapa bagian sepanjang tahun, dengan mempertimbangkan ukuran perusahaan, sumber daya, dan sebagainya.

Namun, simpulan umum di antara semua kasus adalah kewajiban audit internal untuk terus memperjuangkan implementasi dan peningkatan berkelanjutan dari sistem *zero-trust*. Ada berbagai sumber daya di pasar yang membantu tugas ini, berdasarkan elemen yang menjadi fokus model *zero-trust*. Misalnya, mengenai risiko perangkat perusak (*ransomware*), Tirado menggunakan InfraGard, alat berbagi informasi gratis yang dikembangkan melalui kemitraan dengan FBI dan anggota sektor swasta. Hanya dalam beberapa menit di awal setiap hari, Tirado dapat menggunakan alat ini untuk mendapatkan informasi terbaru mengenai serangan *ransomware* terbaru dan pelanggaran data baik di dalam maupun di luar industrinya. "Skala serangan ini memohon pendekatan di luar model keamanan berbasis perimeter," jelasnya. "Memberi tahu pemangku kepentingan tentang seperti apa lingkungan risiko dan apa yang dipertaruhkan adalah prioritas nomor satu audit internal."

Selain itu, penting untuk dicatat bahwa ini bukan transisi yang perlu terjadi sekaligus. "Bahkan dalam bentuk parsial, model *zero-trust* memiliki nilai yang sangat besar," kata Tirado. "Pada akhirnya, model *zero-trust* bermuara di kolom kontrol yang ada di lembar kerja. Mungkin 20, mungkin hanya 10 atau 12. Yah, itu lebih baik dari lima."

Contoh pengendalian sederhana untuk dipertimbangkan pada tahap awal model zero-trust meliputi:

- Enkripsi Data.
- Pelatihan Kesadaran atas Keamanan.
- Rencana Respon Insiden.
- Sistem Deteksi dan Respon Titik Akhir.
- Segmentasi mikro.
- Pemantauan Kepatuhan.
- Analisa Perilaku dan Entitas Pengguna.

Landasan itu Telah Ada

Terlepas dari perubahan inti filosofis di dalam jaringan, auditor internal harus menyadari begitu *zero trust* dipahami, tanggung jawab fungsi itu sendiri tidak boleh sepenuhnya berbeda dari apa yang diharapkan dari mereka sebelumnya. Implementasi *zero-trust* itu sendiri tidak memerlukan perubahan arsitektur atau infrastruktur di luar kemungkinan adopsi peralatan komersial tertentu, begitu pula sistem yang memberikan asurans untuk itu.

Memang, prinsip-prinsip utama dari setiap pekerjaan audit termasuk identifikasi, komunikasi, dan asurans, dan masing-masing tanggung jawab tersebut tetap utuh. Dengan kepemimpinan yang mantap, kepatuhan terhadap Global Internal Audit Standards™, dan kemauan untuk belajar, transisi ke arsitektur jaringan *zero-trust* bukanlah sesuatu yang perlu ditakuti oleh organisasi.

Diterjemahkan dan diselaraskan oleh IIA Indonesia Volunteer:
1. Dyan Garneta Permata Sari, CIA, CRMA
2. Indra Permana, CIA, CRMA
3. Fauzan Wahyuabdi Pratama, CIA, CGAP

Edisi Sebelumnya

Untuk mengakses edisi Perspektif dan Wawasan Global sebelumnya, kunjungi theiia.org/GPI.

Umpan Balik Pembaca

Kirim pertanyaan atau komentar ke globalperspectives@theiia.org.

Tentang IIA

Institute of Internal Auditors (IIA) adalah asosiasi profesional internasional yang melayani lebih dari 255.000 anggota global dan telah memberikan 200.000 sertifikasi Auditor® Internal Bersertifikat (CIA®) di seluruh dunia. Didirikan pada tahun 1941, IIA diakui sebagai pemimpin profesi audit internal dalam standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis di seluruh dunia. Untuk informasi lebih lanjut, kunjungi theiia.org.

Sanggahan

IIA menerbitkan dokumen ini untuk tujuan informasi dan pendidikan. Materi ini tidak dimaksudkan untuk memberikan jawaban pasti atas keadaan individu tertentu dan dengan demikian hanya dimaksudkan untuk digunakan sebagai panduan. IIA merekomendasikan untuk mencari saran ahli independen yang berkaitan langsung dengan situasi tertentu. IIA tidak bertanggung jawab atas siapa pun yang mengandalkan materi ini.

Hak cipta

Hak Cipta © 2025 Institut Auditor Internal, Inc. Semua hak dilindungi undang-undang. Untuk izin untuk mereproduksi, silakan hubungi

copyright@theiia.org. Januari 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101