Risiko positif dalam keamanan siber

AWS Panduan Preskriptif

AWS Panduan Preskriptif: Risiko positif dalam keamanan siber

Table of Contents

Pengantar 1
Manfaat risiko positif 3
Mempromosikan hasil positif 3
Meningkatkan postur keamanan 4
Mengubah bahasa risiko 5
Meningkatkan adopsi 6
Contoh risiko positif 7
Risiko positif teknologi 7
Manajemen proyek risiko positif 7
Risiko positif keamanan siber 7
Respons risiko keamanan siber 9
Langkah selanjutnya 12
Pertanyaan yang Sering Diajukan 13
Risiko naik dan positif 13
Kepentingan 13
Sumber daya 14
Riwayat dokumen 15
..... xvi

Risiko positif dalam keamanan siber

Greg Bell, Amazon Web Services ()AWS

Mei 2022 (riwayat dokumen)

Kebanyakan orang memikirkan risiko dari perspektif negatif, seperti paparan kerugian atau mengelola peristiwa yang merugikan. Namun, definisi risiko Organisasi Internasional untuk Standardisasi (ISO) adalah “efek ketidakpastian pada tujuan.” Dalam hal ini, efeknya mungkin positif atau negatif.

Risiko aktual dapat bervariasi antar industri, tetapi definisi standar ini berlaku untuk semua, dan setiap industri memiliki risiko negatif dan positif. Dalam industri keamanan siber, risiko negatif mengacu pada potensi kerugian, dan risiko positif mengacu pada potensi keuntungan aset, pengetahuan, perbaikan, atau data.

Manajemen proyek dan domain TI telah mengadopsi strategi mengevaluasi risiko positif dalam laporan bisnis dan keputusan bisnis. Namun, industri keamanan siber belum mengadopsi ini sebagai praktik umum, dan banyak metodologi manajemen risiko terus fokus pada risiko negatif. Jika mereka membahas risiko positif sama sekali, itu hanya sebentar.

Secara tradisional, cybersecurity memandang risiko secara eksklusif melalui lensa negatif. Berikut ini adalah dua jenis risiko negatif yang umum dalam keamanan siber:

- Risiko downside — Paparan kerugian dari faktor eksternal, seperti ancaman. Misalnya, penjahat cyber mungkin memperkenalkan atau meningkatkan kemungkinan insiden keamanan.
- Risiko naik — Paparan kerugian saat mengejar keuntungan, seperti kerentanan yang dihasilkan dari perubahan. Misalnya, saat menerapkan strategi TI, Anda mungkin secara tidak sengaja meningkatkan potensi insiden keamanan. Risiko naik tidak sama dengan risiko positif. Meskipun terjadi saat mengejar keuntungan, risiko naik difokuskan pada potensi kerugian.

Sampai saat ini, keamanan siber hanya mempertimbangkan risiko negatif, dan definisi risiko telah difokuskan pada hasil negatif yang potensial. Risiko positif berfokus pada potensi hasil positif pada awal identifikasi risiko. Pengecualian risiko positif mengakibatkan kegagalan untuk mengenali hasil positif dalam keamanan siber. Karena fokus pada risiko negatif, kepemimpinan eksekutif umumnya menganggap cybersecurity reaktif daripada proaktif dan meremehkan kontribusi cybersecurity terhadap hasil bisnis yang positif.

Dokumen ini mendefinisikan risiko positif bagi industri keamanan siber dan membahas manfaat dan pentingnya memasukkan risiko positif dalam strategi keamanan siber Anda.

Manfaat risiko positif

Terutama dalam industri seperti cybersecurity, yang berfokus pada melindungi bisnis dari potensi kerugian, mudah untuk membingkai risiko dari perspektif negatif. Membingkai ulang risiko keamanan siber berdasarkan potensi keuntungan mereka dapat menguntungkan bisnis dengan mempromosikan hasil positif, meningkatkan postur keamanan organisasi, dan meningkatkan kepercayaan pelanggan.

Mempromosikan hasil positif

Mengadopsi risiko positif memungkinkan organisasi untuk mengevaluasi dan mengenali kontribusi domain terhadap hasil bisnis yang positif. Menurut Cybersecurity In The C-Suite and Boardroom (laporan penelitian Enterprise Strategy Group):

- 69% pemimpin bisnis dan teknologi percaya bahwa keamanan siber seluruhnya atau sebagian besar merupakan area teknologi dengan sedikit atau tanpa hubungan dengan bisnis.
- 11% pemimpin bisnis dan teknologi menyamakan keamanan siber dengan kepatuhan terhadap peraturan.
- 82% organisasi mengklaim bahwa risiko keamanan siber telah meningkat selama dua tahun terakhir karena faktor-faktor seperti meningkatnya ancaman siber, integrasi teknologi yang lebih besar dalam bisnis, dan permukaan serangan yang berkembang.

Ketika eksekutif keamanan siber mengintegrasikan risiko positif ke dalam percakapan dan laporan, ini membantu mempromosikan nilai operasi TI yang aman di dalam perusahaan.

Sebagai contoh, katakanlah sebuah bisnis mengalami pelanggaran data beberapa tahun yang lalu, dan pelanggaran data disebabkan oleh kurangnya proses manajemen patch. Insiden ini masih diangkat oleh media, dan itu mempengaruhi persepsi dan interaksi pelanggan dengan perusahaan. Bisnis ingin bergerak melewati insiden dan memperluas penawaran layanan mereka, tetapi kepercayaan pelanggan menghalangi penjualan. Keamanan siber menggunakan risiko positif untuk meyakinkan kepemimpinan untuk berinvestasi dalam proses manajemen patch yang terus memperbarui aplikasi. Proses baru secara dramatis mengurangi risiko pelanggaran data, meningkatkan postur keamanan perusahaan. Berita tentang proses manajemen up-to-the-minute patch menjangkau media dan pelanggan potensial. Pelanggan sekarang merasa nyaman membeli dari bisnis, dan penjualan meningkat ke tingkat yang mengesankan.

Kegagalan untuk mempertimbangkan risiko positif selama identifikasi risiko dapat memberikan penilaian yang tidak lengkap dan mempengaruhi keputusan bisnis. Untuk contoh nyata risiko positif yang dapat memengaruhi keputusan bisnis, lihatContoh risiko positif.

Meningkatkan postur keamanan dan kepercayaan pelanggan

Keamanan siber merupakan bagian integral dari postur keamanan bisnis. Pelanggaran data dapat berdampak negatif pada kepercayaan pelanggan, tetapi postur dan reputasi keamanan yang kuat juga dapat meningkatkan kepercayaan pelanggan dan mendorong peluang bisnis.

Sebagaimana dibahas dalamMempromosikan hasil positif, penelitian menunjukkan bahwa kepemimpinan eksekutif memahami risiko negatif yang terkait dengan keamanan siber tetapi seringkali tidak memahami risiko positif, atau nilai bisnis. Namun, penelitian menunjukkan bahwa kepemimpinan dalam keamanan siber memahami bagaimana postur keamanan yang kuat dapat bermanfaat bagi organisasi.

Dalam Penelitian Keamanan Siber: Akselerator Inovasi (whitepaper Vodafone), Vodafone mewawancarai 1.434 pembuat keputusan di seluruh dunia dalam keamanan siber. Menurut data mereka:

- 73% responden percaya keamanan yang kuat menciptakan peluang bisnis baru.
- 89% mengatakan peningkatan keamanan mereka akan meningkatkan loyalitas dan kepercayaan pelanggan.
- 90% juga mengatakan bahwa mereka mampu meningkatkan citra mereka, menjangkau klien potensial baru, dan juga mengubahnya menjadi klien yang sebenarnya.
- 89% percaya bahwa memiliki keamanan siber yang efektif adalah keunggulan kompetitif yang relevan, yang membantu mereka membedakan dari pesaing mereka.
- 24% melaporkan peningkatan pendapatan dengan menggunakan teknologi cloud dan Internet of Things (IOT) dan dengan mengadopsi kontrol keamanan TI yang ditargetkan.
- Alih-alih menggunakan potensi hasil negatif saat berkomunikasi dengan kepemimpinan eksekutif, Anda juga dapat menggunakan risiko positif untuk mengkomunikasikan nilai bisnis untuk meningkatkan kepercayaan pelanggan. Eksekutif dapat berhati-hati saat mendanai program. Dalam beberapa kasus, keamanan siber mendapatkan minimum yang diperlukan untuk beroperasi. Mengkomunikasikan risiko positif secara internal dalam permintaan pendanaan dapat membantu kepemimpinan Anda memahami nilai bisnis keamanan siber. Hal ini dapat mengakibatkan peningkatan pendanaan untuk inisiatif keamanan siber dan mendorong pendapatan untuk bisnis.

Mengubah bahasa risiko keamanan siber

Bagian dari tantangan mengadopsi risiko positif untuk keamanan siber adalah bahwa terminologi teknis dan domain spesifik difokuskan pada risiko negatif, seperti ancaman, kerentanan, dan kontrol keamanan. Industri keamanan siber harus berkembang dan memperluas kosakata untuk memasukkan bahasa yang menekankan hasil bisnis positif (atau risiko positif) yang dibawa keamanan siber ke bisnis. Ketentuan seperti keuntungan bisnis, manfaat, dan nilai bisnis menyoroti kontribusi keamanan siber bagi organisasi.

Mengubah bahasa keamanan siber membantu mengubah persepsi bahwa keamanan siber adalah area teknologi yang berfokus secara eksklusif pada ancaman dan kerentanan dan bahwa itu tidak terikat dari bisnis. Kepemimpinan bisnis umumnya meremehkan kontribusi keamanan siber terhadap hasil bisnis yang positif. Untuk informasi lebih lanjut tentang persepsi keamanan siber oleh kepemimpinan, lihatMempromosikan hasil positif.

Meningkatkan adopsi di bidang terkait

Ada minat yang berkembang di banyak bidang untuk memasukkan risiko positif karena mengakui kontribusi domain terhadap hasil bisnis. Konsep risiko positif baru-baru ini diadopsi ke dalam proses dan definisi manajemen proyek umum.

Pada tahun 2013, Project Management Institute (PMI) memasukkan definisi risiko positif (juga disebut peluang) ke dalam edisi kelima dari Project Management Body of Knowledge (PMBOK). PMBOK mendefinisikan risiko individu sebagai “peristiwa atau kondisi yang tidak pasti yang, jika terjadi, memiliki efek positif atau negatif pada satu atau lebih tujuan proyek.” Ini mendefinisikan risiko proyek secara keseluruhan sebagai “efek ketidakpastian pada proyek secara keseluruhan... lebih dari jumlah risiko individu dalam suatu proyek, karena mencakup semua sumber ketidakpastian proyek... mewakili paparan pemangku kepentingan terhadap implikasi variasi dalam hasil proyek, baik positif maupun negatif.”

Sayangnya, penyertaan PMI atas hasil positif dalam definisi risikonya belum berlaku untuk industri keamanan siber.

Contoh risiko positif

Berikut ini adalah beberapa contoh risiko positif untuk teknologi, manajemen proyek, dan keamanan siber.

Risiko positif teknologi

Salah satu contoh risiko positif dalam teknologi adalah bahwa penerapan teknologi dapat menyebabkan pengurangan biaya upah. Misalnya:

1. Menerapkan teknologi dapat menghasilkan efisiensi bisnis yang lebih besar.
2. Efisiensi ini dapat menyebabkan pengurangan tenaga kerja.
3. Pengurangan tenaga kerja dapat menyebabkan berkurangnya biaya upah.

Manajemen proyek risiko positif

Salah satu contoh risiko positif dalam manajemen proyek adalah kesalahan perhitungan anggaran proyek dapat menyebabkan penghematan biaya atau pendanaan proyek tambahan. Misalnya:

1. Menerapkan proyek teknologi lebih awal dapat mengakibatkan manajer proyek salah menghitung biaya proyek.
2. Salah menghitung biaya proyek dapat menyebabkan dana proyek yang berlebihan.
3. Dana proyek yang berlebihan dapat menyebabkan penghematan biaya atau pendanaan untuk proyek tambahan.

Risiko positif keamanan siber

Salah satu contoh risiko positif dalam keamanan siber adalah penerapan manajemen patch dapat meningkatkan kepercayaan pelanggan. Misalnya:

1. Menerapkan manajemen patch dapat mengurangi kerentanan dalam aplikasi.
2. Menghapus kerentanan dapat mengurangi risiko aplikasi dan membuat aplikasi lebih aman.
3. Peningkatan keamanan aplikasi dapat mengurangi kehilangan data.
4. Mengurangi kehilangan data dapat meningkatkan kepercayaan pelanggan.

Contoh lain dari risiko positif dalam cybersecurity adalah penerapan respon insiden dapat meningkatkan produktivitas karyawan. Misalnya:

1. Menerapkan respons insiden dapat menyebabkan mendeteksi peningkatan lalu lintas jaringan.
2. Peningkatan lalu lintas jaringan dapat menyebabkan mendeteksi penyalahgunaan sumber daya karyawan dengan mengakses konten yang tidak terkait dengan pekerjaan, seperti layanan streaming musik dan video. Aktivitas ini mengkonsumsi bandwidth jaringan dan dapat berdampak negatif pada kinerja jaringan dan aplikasi.
3. Deteksi penyalahgunaan sumber daya perusahaan oleh karyawan dapat menyebabkan pemblokiran layanan ini.
4. Memblokir layanan ini dapat mengurangi konsumsi bandwidth jaringan dan meningkatkan produktivitas karyawan.

Akhirnya, contoh terakhir dari risiko positif dalam keamanan siber adalah penerapan rencana respons insiden dapat meningkatkan peluang bisnis dan kepatuhan terhadap undang-undang privasi. Misalnya:

1. Menerapkan rencana respons insiden dapat mengarah pada deteksi dan identifikasi malware dan ransomware dengan cepat.
2. Identifikasi malware dan ransomware dapat meminimalkan dampak dan mengurangi ancaman terhadap sumber daya perusahaan.
3. Mengurangi ancaman terhadap sumber daya perusahaan dapat mengarah pada peluang bisnis baru dan membantu bisnis tetap mematuhi undang-undang privasi.

Respons risiko keamanan siber

Respons terhadap risiko positif dan negatif sangat berbeda. Untuk risiko negatif, Anda mengambil langkah-langkah untuk meminimalkan dampak pada hasil, tetapi untuk risiko positif, Anda mengambil langkah-langkah untuk memaksimalkan dampak pada hasil. Tabel berikut menunjukkan respons potensial terhadap risiko positif dan negatif.

Jenis risiko	Respons	Definisi
Risiko positif	Mengeksploitasi	Maksimalkan probabilitas atau kemungkinan risiko yang terjadi untuk mewujudkan efek positifnya.
	Bagikan	Mengalokasikan sebagian dari kepemilikan atau tanggung jawab atas risiko kepada pihak lain. Ini adalah pendekatan yang sama dengan risiko negatif, dan mencoba mengendalikan potensi kerugian atau keuntungan.
	Tingkatkan	Tingkatkan kondisi yang menciptakan risiko untuk memaksimalkan peluang.
	Abaikan	Mengabaikan kemungkinan risiko, dan tidak mengambil tindakan. Respon ini umum terjadi ketika probabilitas risikonya sangat rendah atau ketika manfaat dari potensi hasil positif minimal.

Jenis risiko	Respons	Definisi
Risiko negatif	Mengurangi	Minimalkan probabilitas atau kemungkinan risiko yang terjadi.
	Transfer	Mengalihkan tanggung jawab atau kewajiban atas risiko kepada pihak lain, seperti membeli polis asuransi untuk mentransfer risiko ke perusahaan asuransi.
	Hindari	Hilangkan kondisi yang menciptakan risiko.
	Menerima	Mengakui adanya risiko tetapi tidak mengambil tindakan.

Untuk risiko negatif, organisasi menghindari, mentransfer, mengurangi, atau menerima risiko, berdasarkan toleransi risiko dan selera mereka. Mereka mencoba mencegah risiko terjadi, dan jika itu terjadi, mereka mencoba meminimalkan dampaknya pada misi keseluruhan.

Cara terbaik untuk menggambarkan respons risiko positif adalah dengan menggunakan contoh:

- Seorang eksekutif keamanan mengetahui bahwa seorang profesional keamanan yang berkualitas baru-baru ini memutuskan untuk mencari pekerjaan baru dan mengatur bonus penandatanganan yang murah hati untuk menarik calon karyawan ke timnya.
- Bagikan — Seorang pemimpin unit bisnis ingin meningkatkan keamanan dengan menggunakan produk manajemen akses istimewa tetapi tidak memiliki anggaran yang cukup untuk membeli alat dan layanan pada tahun fiskal berjalan. Pemimpin bekerja dengan pemimpin dari unit bisnis yang berbeda yang akan membeli dan mengimplementasikan alat sebagai proyek percontohan dan kemudian memperluas instalasi untuk mendukung kedua unit bisnis.
- Meningkatkan — Seorang karyawan telah mengidentifikasi peluang untuk mengotomatisasi proses bisnis yang ada untuk mengurangi ancaman keamanan siber, tetapi membutuhkan investasi dalam waktu dan peralatan. Melihat manfaat positif dari proses semacam itu, manajer menyetujui

jam kerja lembur untuk mengembangkan kemampuan dan menggunakan kembali sumber daya perangkat keras dan perangkat lunak yang ada yang memungkinkan proyek untuk melanjutkan.

- Abaikan — Seorang eksekutif keuangan mengetahui bahwa seorang karyawan yang bekerja di departemen penjualan telah mengembangkan aplikasi baru yang mengotomatiskan tugas yang membosankan dan manual. Aplikasi ini baru-baru ini diizinkan untuk digunakan hanya di departemen penjualan. Eksekutif keuangan memperoleh salinan aplikasi baru untuk mendapatkan keuntungan serupa di departemennya, tanpa otorisasi eksplisit.

Langkah selanjutnya

Domain teknologi dan manajemen proyek telah mengadopsi risiko positif ke dalam proses penilaian risiko mereka, tetapi industri keamanan siber secara historis mengecualikannya. Risiko positif dapat menghasilkan hasil bisnis yang positif, dan industri keamanan siber harus bertransisi untuk merangkul risiko positif dan menyadari manfaatnya.

Anda dapat mulai mengkomunikasikan risiko positif segera di semua komunikasi. Misalnya, penilaian risiko, penilaian keamanan, atau laporan status harus mencakup bagian tentang risiko positif. Permintaan pendanaan kepada kepemimpinan eksekutif harus mencakup risiko positif, mengkomunikasikan manfaat potensial bagi bisnis dan menyoroti potensi keuntungan bisnis yang diperoleh dengan menyetujui permintaan tersebut.

Pertanyaan yang Sering Diajukan

Apa perbedaan antara risiko naik dan risiko positif?

Meskipun risiko naik dan risiko positif terdengar serupa, mereka sebenarnya sangat berbeda. Dalam risiko, ada hasil positif atau negatif, dan dalam hasil negatif, ada sisi naik atau turun.

Risiko positif adalah potensi keuntungan dari aset, pengetahuan, perbaikan, atau data. Misalnya, Anda menerapkan manajemen patch dan proses untuk menghapus kerentanan dengan cepat, seperti dalam waktu satu minggu. Selama tahun depan, Anda tidak memiliki insiden keamanan.

Risiko naik adalah paparan kerugian saat mengejar keuntungan. Misalnya, bisnis menyebarkan aplikasi baru, dan Anda menerapkan manajemen patch dan proses untuk menghapus kerentanan dengan cepat, seperti dalam waktu satu minggu. Paparan kerugian (periode waktu ketika Anda menghapus kerentanan) sedang mengejar keuntungan (aplikasi yang lebih aman), jadi ini dianggap sebagai risiko naik. Anda dapat meningkatkan risiko kenaikan dengan mengubah proses untuk menghapus kerentanan menjadi satu hari, atau mengurangi risiko kenaikan dengan mengubah periode menjadi satu bulan. Pada dasarnya, risiko naik adalah kemungkinan keuntungan yang tidak pasti saat mencoba meminimalkan kerugian.

Mengapa penting untuk memasukkan risiko positif dalam keamanan siber?

Mengintegrasikan risiko positif dalam penilaian risiko keamanan siber dan percakapan membantu mempromosikan nilai keamanan siber bagi bisnis. Lihat informasi yang lebih lengkap di Manfaat risiko positif.

Sumber daya

- Keamanan Siber Di C-Suite dan Ruang Rapat (laporan penelitian Grup Strategi Perusahaan)
- Penelitian Keamanan Cyber: Akselerator Inovasi (whitepaper Vodafone)
- Mengintegrasikan Keamanan Siber dan Manajemen Risiko Perusahaan (ERM) (publikasi NIST)
- Mengklarifikasi Risiko “Naik” dan “Positif” (posting blog lembaga FAIR)

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	Mei 27, 2022

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.