**THE IMPACT OF SECURITY TECHNOLOGY ON UNAUTHORIZED PROPERTY TRESPASSING**

PENGARUH TEKNOLOGI KEAMANAN TERHADAP TINDAKAN MASUK PEKARANGAN TANPA IZIN

**Lestyo Ahmad Sidiq**

| ***Abstract*** |
| --- |

*The current digital era positions security as a primary issue. With the rapid pace of digitalization, the protection of personal data becomes essential to prevent illegal actions and privacy breaches. Although laws have been enacted to reinforce digital security in Indonesia, the education of information security to the public is still inadequate. With the development of various security technologies, such as advanced CCTV and motion sensors, there is hope to enhance the protection of property and personal information. However, technology alone is insufficient without public awareness. This study aims to explore the impact of security technologies in confronting unauthorized entries into private areas and emphasizes the necessity of public awareness in safeguarding information security. The research findings indicate that a combination of advanced technology and public awareness is required to create a safe environment.*

***Keywords****: digital security, data protection, security technology, public awareness.*

| **Abstrak** |
| --- |

Era digital saat ini menempatkan keamanan sebagai salah satu isu utama. Dengan percepatan digitalisasi yang terjadi, perlindungan data pribadi menjadi esensial untuk mencegah aksi ilegal dan pelanggaran privasi. Meskipun Undang-Undang telah diterbitkan untuk memperkuat keamanan digital di Indonesia, edukasi keamanan informasi kepada masyarakat masih kurang memadai. Dengan berbagai teknologi keamanan yang dikembangkan, seperti CCTV mutakhir dan sensor gerakan, ada harapan untuk meningkatkan perlindungan terhadap properti dan informasi pribadi. Namun, teknologi sendiri tidak cukup tanpa adanya kesadaran dari masyarakat. Studi ini bertujuan untuk mengeksplorasi dampak teknologi keamanan dalam menghadapi aksi masuk ke area privat tanpa izin dan menekankan perlunya kesadaran masyarakat dalam menjaga keamanan informasi. Hasil penelitian menunjukkan bahwa kombinasi antara teknologi canggih dan kesadaran masyarakat diperlukan untuk menciptakan lingkungan yang aman.

**Kata Kunci :** keamanan digital, perlindungan data, teknologi keamanan, kesadaran masyarakat

1. **PENDAHULUAN**

Dalam era digital yang berkembang pesat, isu keamanan mendapatkan perhatian besar dari berbagai elemen masyarakat, termasuk individu dan organisasi. Perlindungan data pribadi menjadi vital untuk mencegah insiden pelecehan atau intimidasi online. Dikutip dari website Kementerian Keuangan tahun 2020 menyatakan bahwa, Pemerintah Indonesia telah memperkuat landasan hukum keamanan digital melalui Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diperbaharui dengan UU No 19 Tahun 2016. Masyarakat juga diajak untuk meningkatkan literasi digital guna memahami arus informasi di dunia maya. Ini menunjukkan bahwa tanggung jawab keamanan informasi bukan hanya milik pemerintah atau departemen IT dalam suatu organisasi, melainkan tanggung jawab bersama. Sehingga, penggunaan teknologi informasi perlu dilakukan secara bertanggung jawab dengan memastikan etika teknologi tetap terjaga. Percepatan digitalisasi, terutama selama pandemi, mendorong bisnis untuk berinovasi dan bertransisi ke platform digital. Namun, dengan pertumbuhan digitalisasi yang signifikan, edukasi yang belum memadai menjadikan keamanan sebagai tantangan utama (Farizy dan Eriana, 2022). Oleh karena itu, meningkatkan kesadaran dan upaya dalam melindungi teknologi informasi sangat penting di masa kini.

Dalam era modern ini, berbagai teknologi keamanan telah dikembangkan dengan beragam fungsi dan kegunaan. Keamanan Teknologi Informasi berfokus pada perlindungan sistem komputer terhadap ancaman dari pihak-pihak yang tidak memiliki otoritas. Perlindungan data dan sistem mencakup pencegahan terhadap ancaman *cyber*, termasuk akses ilegal, pelanggaran integritas data, infeksi malware, dan sebagainya. Menurut Silalahi (2022), Terdapat berbagai alat dan metode yang diterapkan dalam bidang keamanan informasi, seperti broker keamanan akses *cloud* (CASB), teknik pengamanan komunikasi yang memanfaatkan algoritma tertentu, pemulihan dari kerugian akibat bencana, serta respons terhadap insiden keamanan. Ancaman terhadap keamanan informasi dapat muncul dari sumber yang berbeda, termasuk aktivitas hacker, virus komputer, ketidakstabilan sistem, serta berbagai tindakan kriminal di dunia siber. Beberapa teknik yang sering digunakan untuk mengkompromikan keamanan teknologi informasi meliputi kebocoran data, serangan penolakan layanan (DoS), dan tindakan kriminal lainnya di dunia digital. Jenis-jenis proteksi dalam keamanan teknologi informasi meliputi perlindungan fisik dan lingkungan, mekanisme kontrol akses, serta keamanan dunia maya. Dikutip dari Binus University tahun 2018 menyatakan bahwa, pemanfaatan teknologi keamanan informasi menghadirkan berbagai keuntungan seperti melindungi operasional bisnis, menjaga privasi data, mencegah adware, dan menyediakan lingkungan yang aman untuk para pekerja.

Dalam era teknologi yang terus berkembang, metode pelanggaran keamanan sistem komputer juga semakin canggih. Kejahatan siber merupakan tindakan yang dilakukan dengan sengaja dan terencana untuk merusak, mencuri, atau melakukan tindakan merugikan pada sistem informasi atau komputer (Ngafifi, 2014). Tindakan akses ilegal menggambarkan individu yang sengaja dan tanpa hak mengakses komputer, sistem, atau jaringan yang tidak ditujukan untuk akses publik (Harahap *et al.* 2018). Menurut Tampubolon (2020), hacking adalah taktik untuk memasuki sistem komputer tanpa izin. Penyusupan tanpa otorisasi terjadi ketika seseorang mendapatkan akses ke jaringan komputer tanpa sepengetahuan atau tanpa izin dari pemiliknya. Selanjutnya, pencurian informasi atau data *theft* terjadi ketika data dicuri dari sistem komputer untuk kepentingan pribadi atau dijual ke pihak lain.

Dikutip dari website kominfo tahun 2018, Dalam era digital saat ini, pendidikan dan pelatihan tentang keamanan informasi menjadi esensial untuk meningkatkan kesadaran masyarakat dalam mencegah akses ilegal ke sistem. Melalui edukasi dan sosialisasi, masyarakat dapat memahami signifikansi perlindungan data dan cara memanfaatkan teknologi dengan optimal untuk tujuan keamanan. Sementara itu, menurut laman web Panda pada 2023, dengan pemahaman tersebut, individu dapat mengenali dan menilai risiko serta menentukan tindakan pencegahan yang paling tepat. Edukasi tersebut juga menekankan pada pemahaman mendalam tentang bagaimana teknologi keamanan berfungsi dan strategi terbaik untuk mengimplementasikannya demi mencegah akses tanpa izin. Faktor-faktor seperti menjaga kerahasiaan, memastikan privasi, perlindungan aset bisnis, kepatuhan terhadap regulasi, serta menjaga reputasi perusahaan, semuanya dianggap esensial dan di highlight melalui sosialisasi yang efektif.

Studi ini bertujuan untuk mendalami dampak teknologi keamanan dalam menghadapi aksi masuk ke area privat tanpa izin. Berdasarkan literatur yang telah diteliti, meski di tengah kemajuan ekonomi berbasis digital, aspek perlindungan hukum terhadap privasi tetap menjadi hal yang fundamental mengingat potensi ancaman terhadap privasi dan data pribadi individu. Bentuk kejahatan dunia maya, seperti penyusupan ke dalam sistem komputer tanpa seizin atau sepengetahuan pemiliknya, semakin marak. Teknologi keamanan memainkan peran penting dalam menekan risiko aksi penyusupan ke area privat dengan menyediakan sistem keamanan yang lebih tangguh dan minim celah yang bisa dieksploitasi oleh pelaku. Namun, keberadaan teknologi keamanan tidak menjamin sepenuhnya terhadap aksi penyusupan. Oleh karena itu, kesadaran masyarakat dalam menjaga informasi dan mengadopsi langkah-langkah keamanan tetap sangat diperlukan. Melalui studi ini, diharapkan masyarakat dapat memahami peran penting teknologi keamanan serta perlunya kesadaran dalam menjaga keamanan informasi.

1. **METODE**

Penelitian ini menggunakan metode kualitatif, memungkinkan analisis mendalam terhadap data yang berbasis pada bahasa, baik dari interaksi verbal maupun sumber tertulis. Dengan pendekatan ini, data diinterpretasikan untuk mendapatkan pemahaman mendalam tentang substansinya. Salah satu keunggulan metode ini adalah kemampuan untuk memandang suatu isu dari berbagai perspektif, termasuk mempertimbangkan aspek lingkungan di sekitarnya, membuka kemungkinan menemukan hal-hal yang mungkin terlewat pada pandangan pertama (Robbani dan El Adawiyah, 2023). Tujuan utama penelitian ini adalah untuk memahami peran teknologi keamanan dalam menghalangi tindakan-tindakan yang melanggar batas properti tanpa izin. Dalam rangka mendukung analisis, penelitian ini merujuk pada sumber-sumber seperti regulasi hukum, karya akademik, literatur relevan, dan Kamus Besar Bahasa Indonesia (KBBI). Selanjutnya, analisis diarahkan dengan metode deduktif, di mana kesimpulan diambil dari data yang ada, memberikan perspektif menyeluruh terhadap isu yang diteliti.

1. **HASIL**

Teknologi keamanan di era kontemporer menunjukkan kemajuan yang signifikan dalam mendeteksi dan menghalau akses yang tidak sah. Dukungan dari kecerdasan buatan dan machine learning telah memperkaya kapabilitas sistem ini, memungkinkannya untuk menginterpretasi pola khusus, mengidentifikasi aktivitas yang mencurigakan, dan menyatukan informasi dari sumber-sumber yang berbeda, menjamin respons yang cepat dan tepat terhadap potensi ancaman. Sebagai bagian integral dari keamanan rumahan, sistem CCTV kini menawarkan fitur-fitur canggih seperti kualitas gambar tinggi, deteksi gerakan, dan kemampuan pengenalan wajah. Lebih jauh, beberapa sistem CCTV mutakhir telah terintegrasi dengan layanan cloud, memudahkan pemilik properti untuk memantau situasi dari jarak jauh melalui perangkat mobile. Di sisi lain, alarm pintu dengan sensor magnetisnya menjadi benteng pertama dalam mendeteksi upaya akses tanpa izin, mengaktifkan peringatan saat pintu terganggu. Sementara itu, sensor gerakan kini semakin akurat, dengan kemampuan untuk membedakan antara gerakan hewan dan manusia, meminimalisir risiko kesalahan alarm.

Meskipun teknologi keamanan telah mencapai kemajuan signifikan, masih ada insiden masuk tanpa izin yang terjadi, disebabkan oleh berbagai faktor. Seringkali, titik lemah dalam perangkat keras, isu pada perangkat lunak, atau metode infiltrasi yang belum diketahui menjadi alasan utama. Kesalahan dalam instalasi atau konfigurasi dan keterlambatan dalam pembaruan software juga bisa meninggalkan celah keamanan. Namun, teknologi saja tidak cukup. Kesadaran masyarakat dalam menggunakan teknologi dengan benar, mengizinkan akses dengan hati-hati, dan pemahaman akan potensi ancaman menjadi kunci. Oleh karena itu, kombinasi optimal antara teknologi canggih dan kesadaran pengguna diperlukan untuk menciptakan lingkungan yang aman.

Dalam menerapkan teknologi keamanan, beberapa tantangan seringkali muncul. Pertama, masalah biaya sering menjadi hambatan, tetapi hal ini dapat diminimalkan dengan memulai dari sistem keamanan dasar yang ekonomis dan meningkatkan sejalan dengan kemampuan finansial, atau dengan memanfaatkan program bantuan khusus. Selanjutnya, kompleksitas instalasi bisa menjadi tantangan, namun dengan memilih produk yang *user-friendly* atau menggunakan jasa profesional, instalasi dapat dioptimalkan. Terakhir, pemeliharaan teknologi keamanan memerlukan edukasi berkelanjutan agar masyarakat memahami cara menjaga efisiensi sistem. Namun, penting untuk diingat bahwa teknologi saja tidak cukup. Partisipasi aktif dan kesadaran masyarakat terhadap keamanan adalah esensial. Dengan kombinasi teknologi yang tepat dan kesadaran masyarakat yang tinggi, efektivitas sistem keamanan dapat ditingkatkan.

Di tengah perkembangan teknologi yang pesat, penting bagi masyarakat untuk mengakui kebutuhan akan kesadaran keamanan dan bagaimana teknologi dapat berfungsi sebagai pelindung terhadap ancaman di ranah digital. Teknologi informasi dan komunikasi, meskipun telah membawa kemajuan, jika digunakan tanpa pertimbangan, dapat mempengaruhi karakter anak dan remaja. Ini menekankan pentingnya tuntunan dari keluarga dan orang tua dalam mengajarkan penggunaan teknologi dengan cara yang aman dan bijaksana. Selanjutnya, penelitian telah mengindikasikan bahwa masyarakat Indonesia, pada umumnya, masih kurang sadar akan pentingnya keamanan siber. Ini menunjukkan kebutuhan mendesak bagi pemerintah untuk mendorong peningkatan kesadaran keamanan dan memperkuat pertahanan sistem informasi kita. Di sisi lain, adopsi teknologi telah menyebabkan penurunan interaksi sosial, mengakibatkan rasa ketidakpercayaan di antara individu. Masyarakat harus menyadari nilai interaksi sosial yang nyata dan mempertimbangkan kembali ketergantungan mereka pada teknologi. Terakhir, menumbuhkan kesadaran bela negara, sebagaimana diamanatkan oleh undang-undang, adalah esensial dalam memastikan keamanan dan pertahanan negara kita, terutama di tengah tantangan kontemporer.

Keamanan pekarangan yang optimal memerlukan pendekatan komprehensif yang mencakup teknologi, kesadaran pribadi, dan kolaborasi masyarakat. Mengandalkan teknologi semata mungkin tidak memberikan hasil yang diinginkan karena adanya potensi kelemahan teknologi yang bisa dieksploitasi oleh para penjahat. Dengan demikian, pendekatan yang mengintegrasikan kesadaran pribadi serta kolaborasi komunitas menjadi krusial untuk menghindari pelanggaran seperti masuk tanpa izin. Sebagai ilustrasi, pertimbangkan keamanan siber sebuah korporasi. Memastikan keamanan digital korporasi memerlukan pendekatan menyeluruh di mana setiap entitas dalam perusahaan memegang tanggung jawab dalam menjaga keamanan sistem. Namun, mengimplementasikan pendekatan semacam itu seringkali menantang, seperti tercermin dari meningkatnya insiden serangan siber terhadap entitas bisnis. Pandangan menyeluruh terhadap keamanan nasional juga mengemphasiskan pentingnya memahami dan menerapkan keamanan dari sudut pandang yang lebih luas. Ini merupakan perluasan dari tiga aspek keamanan yang biasanya diterima: keamanan politik, domestik, dan militer. Dengan melampaui ketiga domain tradisional tersebut, keamanan nasional kini melibatkan domain-domain tambahan, memberikan jaminan yang lebih komplet dan memungkinkan pendekatan yang lebih adaptif dalam melindungi kepentingan utama negara dan rakyatnya. Untuk mempertahankan keamanan pekarangan, pendekatan komprehensif melibatkan penggunaan teknologi, seperti kamera pengawas, alarm, dan sensor pergerakan, dipadukan dengan edukasi individu dan inisiatif masyarakat. Meningkatkan kesadaran individu bisa dilakukan dengan edukasi mengenai keamanan digital dan penggunaan teknologi dengan bijak. Sementara itu, kolaborasi komunitas mungkin melibatkan pembentukan kelompok pengawas lingkungan yang saling memantau dan melaporkan aktivitas yang mencurigakan.

Dalam era yang ditandai oleh kemajuan teknologi, ada potensi besar untuk meningkatkan keamanan melalui inovasi. Sebagai contoh, teknologi biometrik, seperti sistem pengenalan wajah dan sidik jari, menawarkan identifikasi individu yang lebih presisi. Sementara itu, blockchain menjanjikan integritas data yang lebih tinggi, dan AI serta machine learning berfungsi untuk mengenali tindakan mencurigakan dengan lebih cepat dan efisien. Selain itu, dengan bantuan Internet of Things (IoT), individu dapat terhubung dengan alat keamanan di rumah mereka dari lokasi manapun. Namun, untuk mengoptimalkan keamanan, diperlukan sinergi antara berbagai pihak: masyarakat, pemerintah, dan industri. Pemerintah, misalnya, bisa memberi insentif atau bantuan finansial untuk mendorong masyarakat dan pelaku bisnis kecil memanfaatkan teknologi keamanan. Di sisi lain, sektor industri memiliki peran penting dalam menciptakan solusi keamanan yang efisien dan ekonomis. Sedangkan masyarakat, sebagai pengguna akhir, harus dilibatkan dalam pelatihan dan edukasi untuk memaksimalkan manfaat dari teknologi tersebut. Adopsi teknologi keamanan yang inovatif, dikombinasikan dengan kesadaran masyarakat, dapat membentuk pertahanan yang solid terhadap berbagai risiko. Meskipun teknologi memegang kunci penting, pendekatan yang menyeluruh mengintegrasikan teknologi, pemahaman individu, dan kerja sama lintas sektor adalah kunci untuk menciptakan lingkungan yang aman.

1. **PEMBAHASAN**
2. **Tinjauan Teknologi Keamanan**

Teknologi keamanan terus berkembang dan memberikan perlindungan yang semakin optimal terhadap area tertentu. Namun, teknologi keamanan harus terus mempersiapkan diri menghadapi metode-metode baru yang diterapkan oleh pelaku kejahatan. Oleh karena itu, adaptasi dan pembaruan teknologi keamanan adalah hal yang krusial. Dalam menghadapi strategi yang senantiasa berkembang dari pelaku kejahatan, teknologi keamanan perlu selalu diperbarui dan disesuaikan. Dengan pelaku yang terus-menerus menciptakan taktik baru untuk melanggar keamanan, penting bagi teknologi untuk selalu satu langkah di depan. Untuk mencapai hal ini, kolaborasi erat antara masyarakat, pemerintah, dan sektor industri diperlukan guna merancang dan menerapkan solusi keamanan yang lebih maju dan responsif (Ahadiat, 2010).

Selain itu, teknologi keamanan juga harus mempertimbangkan adanya perubahan taktik dan strategi dalam perjuangan pelaku kejahatan. Pelaku kejahatan dapat menggunakan teknologi komunikasi dan informasi modern untuk menyebarkan fundamentalisme, ekstremisme, dan propaganda. Oleh karena itu, teknologi keamanan harus mampu memperbarui taktik dan strategi serta memperluas komponen organisasi untuk menghadapi ancaman tersebut.

1. **Analisis Efektivitas Teknologi**

Walaupun teknologi keamanan terus mengalami kemajuan, masih mungkin terjadi tindakan masuk tanpa izin karena celah-celah keamanan yang ada dalam teknologi tersebut. Beberapa potensi celah keamanan mencakup aspek manusia dan teknologi itu sendiri. Salah satu faktor risiko yang sering terjadi adalah kesalahan manusia dalam berinteraksi dengan teknologi. Sebagai contoh, dalam insiden serangan terhadap *SingHealth*, para penyerang berhasil memperoleh akses ke sistem melalui eksploitasi terhadap kelemahan dalam workstation sisi depan. Di samping itu, kerentanan dalam teknologi keamanan juga menjadi perhatian penting, karena penyerang dapat memanfaatkan kerentanan tersebut untuk melakukan tindakan tanpa izin. Oleh karena itu, pengujian keamanan secara berkala sangat diperlukan untuk mengidentifikasi dan mengatasi potensi kerentanan (Farizy dan Eriana, 2022).

Pentingnya menyatukan teknologi dan kesadaran manusia dalam menjaga keamanan telah menjadi perhatian utama bagi berbagai organisasi. Untuk meningkatkan kesadaran keamanan, langkah-langkah seperti pelatihan dan sosialisasi kepada masyarakat tentang penggunaan teknologi informasi dan perlindungan data menjadi langkah awal yang sangat penting. Selain itu, membentuk tim IT yang memiliki tanggung jawab untuk mengelola sistem informasi dan menjaga keamanan data juga merupakan bagian penting dalam menjaga keamanan secara keseluruhan. Pengembangan aplikasi dan sistem informasi yang sesuai dengan kebutuhan masyarakat dapat membantu dalam menciptakan lingkungan teknologi yang lebih aman. Terakhir, penggunaan kata sandi yang kuat, yang mencakup kombinasi huruf, angka, dan karakter khusus, juga merupakan praktik penting dalam meningkatkan keamanan teknologi (Nist, 2020). Dalam upaya menjaga keamanan secara menyeluruh, perlu memperhatikan tiga aspek utama, yaitu orang, proses, dan teknologi. Selain itu, pengembangan desa digital yang berfokus pada inklusi keamanan data dapat memastikan bahwa teknologi menjadi aksesible bagi semua lapisan masyarakat, termasuk yang paling rentan terhadap ancaman siber.

1. **Tantangan dalam Penerapan Teknologi Keamanan**
2. **Kendala Biaya**

Menurut Pranowo (2020), dalam era digital saat ini, investasi dalam teknologi keamanan menjadi sebuah kebutuhan yang sering membutuhkan alokasi dana yang cukup besar, khususnya untuk perangkat keras, lunak, dan infrastruktur pendukung. Banyak masyarakat merasa terbebani dengan biaya awal yang tinggi ini. Namun, ada beberapa cara untuk mengatasi masalah ini. Sebagai contoh, dengan melakukan penelitian mendalam, masyarakat dapat menemukan alternatif keamanan yang efisien namun tetap ekonomis. Selain itu, mempertimbangkan cara-cara seperti skema pembiayaan atau penyewaan mungkin dapat menjadi opsi yang menarik untuk mengurangi tekanan biaya di awal.

1. **Masalah Pemasangan**

Menurut Farizy dan Eriana (2022), teknologi keamanan khususnya yang memiliki kompleksitas tinggi, bisa menimbulkan tantangan tersendiri saat proses pemasangan, terutama ketika harus diintegrasikan dengan sistem yang sudah ada sebelumnya. Pemasangan yang kurang tepat dapat mengurangi efektivitas dari teknologi keamanan tersebut. Oleh karena itu, salah satu solusi yang bisa diambil adalah dengan melibatkan pakar atau profesional di bidang keamanan digital saat proses pemasangan berlangsung. Selain itu, memilih teknologi keamanan yang relatif lebih sederhana dalam hal instalasi dan konfigurasi bisa menjadi pilihan yang bijaksana bagi mereka yang kurang berpengalaman dalam hal ini.

1. **Pemeliharaan**

Setiap teknologi, termasuk teknologi keamanan, memerlukan pemeliharaan berkala agar dapat berfungsi dengan optimal. Pemeliharaan ini bisa mencakup berbagai hal, mulai dari pemantauan, pembaruan perangkat lunak, hingga perbaikan teknis saat diperlukan. Tentunya, hal ini bisa menjadi beban tambahan, baik dari sisi waktu maupun biaya. Untuk memastikan bahwa teknologi keamanan tetap berjalan dengan baik, masyarakat disarankan untuk menetapkan rutinitas pemeliharaan yang konsisten. Melibatkan profesional dalam proses pemeliharaan dan reparasi juga dapat menjadi solusi untuk menghindari kerusakan mendadak dan beban biaya yang tidak terduga.

Menghadapi kendala-kendala di atas memang memerlukan usaha dan strategi khusus. Namun, dengan komitmen yang kuat, masyarakat dapat memastikan bahwa teknologi keamanan yang mereka terapkan dapat memberikan perlindungan yang maksimal untuk aset dan informasi penting mereka.

1. **Respons Masyarakat dan Kesadaran Keamanan**

Tingkat kepercayaan masyarakat terhadap teknologi, khususnya dalam aspek keamanan dan perlindungan data, telah menunjukkan pertumbuhan signifikan. Beberapa elemen yang mempengaruhi kepercayaan ini meliputi:

* Pengetahuan dan Kesadaran akan Keamanan: Kepercayaan terhadap teknologi biasanya lebih tinggi di kalangan masyarakat yang teredukasi dan sadar akan keamanan. Dengan pemahaman yang mendalam mengenai risiko-risiko keamanan, masyarakat akan lebih cermat dalam melindungi informasi pribadi mereka.
* Dampak Teknologi pada Kehidupan Sosial: Teknologi telah membawa berbagai perubahan dalam komunikasi dan interaksi sosial. Meskipun mempercepat komunikasi, teknologi juga menimbulkan ancaman, seperti *cyberbullying* dan pelanggaran privasi oleh entitas tak bertanggung jawab. Hal ini tentunya berdampak pada persepsi kepercayaan masyarakat terhadap teknologi.
* Peranan Media Sosial: Media sosial, dengan perkembangannya yang pesat, berperan besar dalam membentuk persepsi masyarakat mengenai teknologi. Dengan kemudahan akses informasi, masyarakat harus bijaksana dalam memfilter informasi dan sadar akan pentingnya keamanan dalam beraktivitas di dunia maya.
* Kerjasama Multipihak untuk Edukasi: Untuk memperkuat kepercayaan dan kesadaran masyarakat terhadap teknologi, kerjasama antara pemerintah, institusi pendidikan, dan komunitas sangat diperlukan. Melalui pendidikan keamanan dan pelatihan, masyarakat akan lebih terinformasi mengenai prinsip-prinsip keamanan siber dan bagaimana melindungi diri di era digital.

Dengan meningkatnya kesadaran akan pentingnya keamanan siber, diharapkan masyarakat dapat memanfaatkan teknologi dengan lebih aman dan bertanggung jawab.

1. **Pendekatan Holistik dalam Keamanan Pekarangan**

Menurut Hamid (2018), Mengandalkan teknologi semata dalam hal keamanan pekarangan bukanlah solusi yang efektif. Meski teknologi mampu menawarkan banyak keunggulan, seringkali ada keterbatasan dan potensi celah yang dapat dieksploitasi oleh pihak yang bermaksud buruk. Selain potensi kerusakan atau kegagalan teknologi, ada kemungkinan bahwa teknologi dapat ditembus oleh mereka yang memahaminya dengan mendalam. Oleh karena itu, pendekatan yang lebih luas diperlukan.

Kesadaran setiap individu memegang peranan krusial. Pemahaman tentang risiko dan langkah-langkah pencegahan masuk tanpa izin sangat penting. Sebagai contoh, masyarakat yang teredukasi akan lebih proaktif melaporkan aktivitas mencurigakan, sehingga mencegah potensi ancaman. Selain itu, kerjasama antar anggota komunitas dapat meningkatkan efektivitas pengawasan dan pencegahan. Keberadaan komunitas yang saling berkomunikasi dan bekerja sama untuk mengawasi lingkungannya membuat upaya pencegahan menjadi lebih kuat (Paripurno dan Jannah, 2014).

Menurut Nasional dan Pembangunan (2013), Beberapa kasus telah membuktikan efektivitas pendekatan holistik ini. Sebagai contoh, Program *Neighborhood Watch* telah terbukti sukses. Dalam program ini, anggota komunitas aktif memantau lingkungannya dan melaporkan hal-hal mencurigakan. Pendekatan serupa juga diterapkan pada sistem keamanan pintu gerbang, yang tidak hanya bergantung pada kamera dan sensor gerakan tetapi juga keterlibatan dan kesadaran masyarakat sekitar. Program pengawasan lingkungan adalah contoh lain dimana masyarakat berkolaborasi untuk memastikan keamanan bersama, yang didukung oleh pendidikan keamanan yang sesuai.

1. **Rekomendasi untuk Masa Depan**

Di masa mendatang, kemajuan teknologi keamanan menjadi hal yang sangat penting. Perusahaan teknologi ternama seperti Google kini memprioritaskan inovasi mereka pada teknologi keamanan yang dirancang untuk melindungi data dan privasi pengguna secara otomatis. Ini termasuk memberikan lapisan perlindungan tambahan bagi mereka yang berada dalam risiko tinggi. Selain itu, dalam upaya mengendalikan penyebaran COVID-19, kolaborasi antara Google dan Apple telah menghasilkan teknologi pelacakan kontak yang menempatkan privasi dan keamanan sebagai prioritas. Dalam konteks urban, pemerintah daerah mengeksplorasi cara-cara untuk mengintegrasikan teknologi cerdas guna meningkatkan efisiensi birokrasi dan pelayanan masyarakat.

Namun, teknologi sendiri tidak cukup. Masyarakat memerlukan pemahaman mendalam tentang teknologi dan potensi risikonya. Untuk itu, kerjasama antara pemerintah dan sektor swasta dalam memberikan pendidikan dan pelatihan keamanan menjadi sangat krusial. Menurut website Kementerian Perindustrian (2021), sinergi antara pemerintah dan industri perlu ditingkatkan. Sebagai contoh, Kementerian Perindustrian telah memulai inisiatif untuk menggandeng IKM dan perusahaan startup, dengan tujuan menciptakan solusi teknologi yang memenuhi kebutuhan kedua belah pihak. Dan yang tak kalah pentingnya, masyarakat harus aktif terlibat dalam upaya keamanan, termasuk dalam aspek-aspek seperti keamanan pangan dan keamanan lingkungan rumah (Taufik *et al.* 2021). Setiap individu perlu memiliki kesadaran dan tanggung jawab dalam menjaga keamanan lingkungannya.

1. **KESIMPULAN**

Keamanan digital kini menjadi unsur kritikal dalam dunia yang semakin berbasis teknologi. Seiring dengan evolusi metode ancaman, teknologi keamanan harus terus berinovasi dan memastikan keandalannya. Meskipun memberikan banyak kelebihan, terdapat beberapa hambatan seperti kesalahan pengguna dan potensi kerentanan teknologi. Oleh sebab itu, evaluasi keamanan berkelanjutan menjadi hal yang penting. Meski investasi di bidang keamanan mungkin membutuhkan biaya yang tidak sedikit, dengan strategi yang tepat, solusi yang hemat biaya dapat dicapai. Kolaborasi antara berbagai entitas, seperti pemerintah, dunia usaha, dan masyarakat umum, dinyatakan penting dalam berbagai kajian. Kesadaran perorangan sangat menentukan, dan pendekatan yang menggabungkan teknologi dengan keterlibatan masyarakat dianggap paling efisien. Kepercayaan publik terhadap teknologi keamanan meningkat seiring dengan peningkatan pemahaman tentang pentingnya keamanan. Namun, edukasi dan latihan masih menjadi fondasi utama dalam mengembangkan kesadaran tersebut. Ke depannya, kerja sama antara sektor pemerintah dan swasta, dengan dukungan masyarakat, sangat penting dalam menavigasi isu-isu keamanan di zaman digital. Sebagai saran, pendekatan komprehensif yang mengkombinasikan teknologi, edukasi, dan kolaborasi lintas sektor harus senantiasa diperkuat untuk membangun lingkungan digital yang lebih aman bagi semua pihak.

DAFTAR PUSTAKA

Ahadiyat, A. (2010). Manajemen Strategik Tinjauan Teoritikal Multiperspektif (Edisi Kesatu). *Bandar Lampung: Penerbit Universitas Lampung.*

Farizy, S., & Eriana, E. S. (2022). Keamanan Sistem Informasi

Harahap, B. A., Paundralingga, A. Y., Kusuma, A. C. M., Harahap, B. A., & Paundralingga, A. Y. (2018). Implikasi Makroekonomi Dari Inovasi Digital: Studi Literatur. *Occasional Paper*.

Hamid, H. (2018). Manajemen pemberdayaan masyarakat.

Nasional, B. P. P., & Pembangunan, B. P. (2013). Masyarakat Adat di Indonesia: Menuju Perlindungan Sosial yang Inklusif. *Kementrian PPN/Bappenas*, 1-144.

Ngafifi, M. (2014). Kemajuan teknologi dan pola hidup manusia dalam perspektif sosial budaya. *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, *2*(1).

Nofalia, I. (2018). Modul Pembelajaran S1 Keperawatan Semester 5.

Paripurno, E. T., Jannah, E. T. (2014). Panduan Pengelolaan Risiko Bencana Berbasis Komunitas (PRBBK).

Pranowo, I. D. (2020). Sistem Dan Manajemen Pemeliharaan (Maintenance. System Dan Management.

Robbani, H., & El Adawiyah, S. (2023). Brand Strategy Lembaga Amil Zakat (LAZ) Zakat Sukses. *Madani: Jurnal Ilmiah Multidisiplin*, *1*(7).

Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1-285.

Tampubolon, M. P. (2020). Change Management: Manajemen Perubahan: Individu, Tim Kerja, Organisasi.

Taufik, A., Chaminra, T., Utami, I. R., Isnaad, A. D. P., Gaffar, D. E., & Rusman, M. (2021). Strategi Pemerintah Dalam Meningkatkan Ketahanan Pangan Pada Masa Pandemi Di Kabupaten Majene. *Kybernology: Journal of Government Studies*, *1*(2), 178-194.