JUSTIFY: Jurnal Sistem Informasi Ibrahimy
Vol. 2, No. 2, Januari 2024, hal. 178-181
E-ISSN: 2962-3642 | P-ISSN: 2962-3871
DOI: 10.35316/justify.v2i2.4159

Identifikasi Kerentanan dan Upaya untuk Melindungi Data Pada Aplikasi Seluler

Abdul Karim[1*], Muhammad Nahidhul Umam[1], Muhammad Lutfi Fatahillah[1], Moh. Aldy Fermansyah Hadi[1]
[1]Teknik Informatika, Universitas Nurul Jadid, Probolinggo, Indonesia

Info Artikel

Riwayat Artikel:
Diterima : **20-11-2023**
Direvisi : **02-01-2024**
Disetujui : **14-01-2024**

Kata Kunci:
Aplikasi
Seluler
Keamanan data

ABSTRAK

Keamanan Aplikasi Seluler mengacu pada upaya untuk melindungi aplikasi yang dijalankan pada perangkat seluler (seperti smartphone atau tablet) dari ancaman keamanan dan potensi risiko yang dapat membahayakan pengguna, data pribadi, dan perangkat itu sendiri. Identifikasi kerentanan pada aplikasi seluler merujuk pada proses pengenalan dan analisis potensi celah keamanan atau kelemahan dalam suatu aplikasi seluler. Tujuan dari identifikasi kerentanan ini adalah untuk menemukan dan memahami potensi risiko keamanan yang dapat dieksploitasi oleh pihak yang tidak sah, seperti peretas atau penyerang. Agar pengguna seluler selalu waspada dan berupaya dalam melindungi data pribadi yang ada pada aplikasi seluler. Dari hasil penelitian yang melibatkan anggota PKK desa Alassumur Besuk Probolinggo bahwa beberapa bentuk kejahatan yang melibatkan seluler dan yang paling umum terjadi bagi pengguna sesluler adalah kurangnya enkripsi data yang memadai, penggunaan kata sandi yang lemah, serta masalah keamanan jaringan yang mungkin memungkinkan penyerang untuk mengakses data sensitif. Hal ini terjadi karena sebagian responden yaitu ibu-ibu PKK masih awam dengan teknologi, sehingga dari penelitian ini dihasilkan langkah-langah atau upaya bagaimana cara melindungi data pribadi khususnya yang terkait dengan seluler.

***Keywords*:**

Application
Cellular
data security

ABSTRACT

Mobile Application Security refers to efforts to protect applications running on mobile devices (such as smartphones or tablets) from security threats and potential risks that could harm users, personal data, and the devices themselves. Vulnerability identification in mobile applications refers to the process of identifying and analyzing potential security gaps or weaknesses in a mobile application. The goal of vulnerability identification is to discover and understand potential security risks that could be exploited by unauthorized parties, such as hackers or attackers. So that mobile users are always alert and make efforts to protect personal data in mobile applications. From the results of research involving PKK members in Alassamur Besuk village, Probolinggo, it is clear that several forms of crime involving cellular and the most common among cellular users are the lack of adequate data encryption, the use of weak passwords, and network security problems that might allow attackers to access data. sensitive. This happened because some of the respondents, namely PKK women, were still unfamiliar with technology, so this research resulted in steps or efforts on how to protect personal data, especially those related to cellular.

Penulis Korespondensi:

Abdul Karim,
Teknik Informatika,
Universitas Nurul Jadid
Email: karimsttnj@gmail.com

1. PENDAHULUAN

Seiring dengan meningkatnya popularitas aplikasi seluler, masalah keamanan juga meningkat. Peningkatan mobilitas organisasi biasanya mengakibatkan peningkatan jumlah perangkat seluler yang mengakses sistem dari jauh. Kerentanan aplikasi seluler dapat menyebabkan kehilangan data dalam jumlah besar, risiko informasi pribadi, dan banyak lagi. Hal ini menyiratkan peningkatan jumlah titik akhir dan beberapa risiko untuk mengamankan dan mencegah pelanggaran data.

Saat ini, masyarakat semakin melek dengan teknologi. Setiap saat pasti berhubungan dengan teknologi komunikasi dan informasi. Meski demikian, pesatnya teknologi digital juga membawa dampak negatif. Salah satunya ialah adanya ancaman terhadap keamanan data pribadi kita. Jika data pribadi tersebut jatuh ke tangan yang salah, maka bisa saja digunakan untuk melakukan tindakan kriminal seperti pencurian identitas atau penipuan. Maka dari itu, perlindungan data pribadi menjadi sangat penting di era digital seperti sekarang ini.

Adanya Kejahatan Siber (cybercrime) telah menjadi ancaman diberbagai kehidupan manusia, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet. Hal ini merupakan akibat dari pesatnya perkembangan teknologi informasi, sehingga setiap perkembangan pada hakikatnya membawa dampak yang positif maupun negatif. Salah satu dampak negatifnya adalah adanya penyalahgunaan data dan informasi pribadi. Kelemahan dunia siber tidak terlepas dari kurangnya pengaturan atau belum adanya regulasi mengenai kemanan siber dan perlindungan data pribadi, sehingga menimbulkan kerancauan ditengah-tengah anggota masyarakat. (Ririn Aswandi dkk,2020)

Keamanan Aplikasi Seluler mengacu pada upaya untuk melindungi aplikasi yang dijalankan pada perangkat seluler (seperti smartphone atau tablet) dari ancaman keamanan dan potensi risiko yang dapat membahayakan pengguna, data pribadi, dan perangkat itu sendiri. Dalam era yang semakin terhubung dan digital, aplikasi seluler telah menjadi bagian integral dari kehidupan kita, dan dengan semakin banyaknya aplikasi yang digunakan, penting untuk memastikan bahwa aplikasi tersebut aman dari serangan dan penyalahgunaan.Keamanan data menjadi hal yang sangat penting pada saat ini karena untuk setiap pengambilan keputusan, kebijakan harus berdasarkan data. Banyak data yang berisikan informasi penting dan terbatas untuk diketahui pihak yang terkait saja (Pratiwi, 2016).

Melindungi data pada seluler adalah tugas penting dalam menjaga keamanan informasi pribadi dan bisnis. Ada beberapa upaya yang dapat dilakukan untuk melindungi data dari serangan phishing diantaranya 1) Kesadaran Pengguna: Memberikan pelatihan dan edukasi kepada semua pengguna tentang apa itu phishing, bagaimana cara mengidentifikasi pesan singkat,email atau situs web phishing, dan apa yang harus dilakukan jika mereka menerima pesan singkat, email atau tautan yang mencurigakan. 2) Verifikasi Pengirim: Selalu verifikasi pengirim email sebelum mengklik tautan atau memberikan informasi sensitif. Periksa alamat email secara seksama, termasuk domainnya. 3) Hindari Tautan Langsung: Hindari mengklik tautan langsung yang diterima melalui email atau pesan instan. Semakin berkembangnya media sosial maka masalah keamanan informasi dan privasi juga menjadi hal yang penting saat ini (Mesra dkk, 2022).

Identifikasi kerentanan pada aplikasi seluler merujuk pada proses pengenalan dan analisis potensi celah keamanan atau kelemahan dalam suatu aplikasi seluler. Tujuan dari identifikasi kerentanan ini adalah untuk menemukan dan memahami potensi risiko keamanan yang dapat dieksploitasi oleh pihak yang tidak sah, seperti peretas atau penyerang. Agar pengguna seluler selalu waspada dan berupaya dalam melindungi data pribadi yang ada pada aplikasi seluler.

2. METODE PENELITIAN

Pada penelitian ini adalah menggunakan metode studi kasus dimana metode studi kasus adalah pendekatan penelitian yang mendalam dan mendetail terhadap suatu kasus tunggal atau sekelompok kasus yang kompleks. Metode ini menggambarkan secara mendalam situasi atau fenomena tertentu dengan mengumpulkan data dari berbagai sumber, seperti observasi, wawancara, analisis dokumen, atau kombinasi dari teknik-teknik tersebut. Tujuan dari metode studi kasus adalah untuk memahami kasus secara menyeluruh, menggali informasi mendalam, dan mendapatkan wawasan yang lebih mendalam tentang permasalahan atau fenomena yang sedang diteliti. Metode studi kasus berfokus pada kasus tunggal atau sekelompok kasus yang spesifik. Kasus tersebut dapat berupa individu, kelompok, organisasi, lokasi, atau fenomena tertentu yang menarik untuk diteliti. Metode studi kasus umumnya menggunakan pendekatan kualitatif dalam pengumpulan dan analisis data. Ini berarti peneliti berusaha untuk memahami konteks, makna, dan interpretasi dari perspektif partisipan dan melibatkan diri secara mendalam dalam studi tersebut.Penelitian ini menggunakan berbagai teknik pengumpulan data untuk mendapatkan pemahaman yang mendalam tentang kasus. Ini bisa meliputi wawancara dengan informan kunci, observasi langsung, analisis dokumen, dan catatan lapangan. Penelitian studi kasus merupakan penelitian, penyelidikan atau pemeriksaan secara mendalam, terperinci, dan detail terhadap suatu peristiwa atau fenomena yang terjadi dalam suatu lingkungan. Hal tersebut sebagaimana yang dibahas dalam buku berjudul Studi Kasus Keperawatan; Pendekatan Kualitatif yang ditulis oleh Aziz Alimul Hidayat *(2021)*. Menurut Susilo Rahardjo

dan Gudnanto (2011), penelitian studi kasus adalah metode yang diterapkan untuk memahami individu lebih mendalam dengan dipraktekkan secara integratif dan komprehensif. Langkah tersebut dilakukan untuk memahami karakter individu yang diteliti secara mendalam.Menurut Bimo Walgito (2010), metode studi kasus adalah metode yang bertujuan untuk mempelajari dan menyelidiki suatu kejadian atau fenomena mengenai individu, seperti riwayat hidup seseorang yang menjadi objek penelitian.

Salah satu contoh kasus kejahatan yang melibatkan aplikasi seluler adalah kasus *phishing* yang marak terjadi pada saat ini, di mana korban dari pencurian data tersebut adalah pengguna aplikasi seluler. Beberapa kasus phishing yang trens saat ini adalah pencurian data melalui pesan singkat yang dikirim melalui pesan singkat whatsapp dengan file apk ataupun pdf. Melalui penelitian ini akan uraikan tentang identikasi kerentanan keamanan aplikasi seluler serta bagaimana melindungi data, baik data pribadi maupun data perusahaan.

3. HASIL DAN ANALISIS

Penelitian ini adalah penelitian studi kasus dengan judul Keamanan Aplikasi Seluler: Identifikasi Kerentanannya dan Upaya untuk Melindungi Data. Menurut Tony Dwi Susanto yang menulis tentang Metode Penelitian Studi Kasus (2020) menjelaskan bahwa studi kasus adalah sebuah penelitian tentang suatu peristiwa yang telah terjadi tanpa si peneliti melakukan intervensi apapun. Dari beberapa jenis penelitian studi kasus penelitian yang sedang dilakukan merupakan penelitian studi kasus deskriptif. Penelitian deskriptif adalah metode yang dilakukan untuk meneliti status kelompok, manusia, objek, suatu set kondisi, sistem pemikiran ataupun suatu kelas peristiwa pada masa sekarang. Tujuan penelitian ini untuk membuat deskriptif atau gambaran secara sistematis, aktual dan akurat mengenai fakta-fakta, sifat serta hubungan antar fenomena yang diselidiki. Deskriptif mempelajari aspek sosial atau masalah-masalah dalam masyarakat, serta norma yang berlaku di dalam masyarakat, termasuk hubungan, kegiatan, sikap, pandangan, proses yang sedang berlangsung, dan pengaruh dari peristiwa tersebut.

Dari hasil penelitian yang melibatkan anggota PKK desa Alassumur Besuk Probolinggo bahwa beberapa bentuk kejahatan yang melibatkan seluler dan yang paling umum terjadi bagi pengguna sesluler adalah kurangnya enkripsi data yang memadai, penggunaan kata sandi yang lemah, serta masalah keamanan jaringan yang mungkin memungkinkan penyerang untuk mengakses data sensitif. Dari hasil penelitian juga menemukan bahwa sebagian besar pengguna tidak cukup sadar akan praktik keamanan yang baik ketika menggunakan aplikasi seluler. Serta yang banyak menimpa masyarakat awam adalah iming-iming hadiah yang menggiurkan yang disampaikan penipu dunia maya kepada korbannya. Hal ini terjadi karena sebagian responden yaitu ibu-ibu PKK masih awam dengan teknologi, sehingga dari penelitian ini dihasilkan langkah-langah atau upaya bagaimana cara melindungi data pribadi khususnya yang terkait dengan seluler.

4. KESIMPULAN

Berdasarkan hasil penelitian tentang identifkasi kerentanan dan upaya melindungi data pada aplikasi seluler maka dapat diambil beberapa kesimpulan diantaranya:

1. Aplikasi Seluler Rentan terhadap Ancaman Keamanan: Penelitian menunjukkan bahwa banyak aplikasi seluler rentan terhadap berbagai ancaman keamanan, seperti peretasan, pencurian data, dan serangan malware. Hal ini disebabkan oleh kerentanannya terhadap berbagai jenis serangan, termasuk serangan sumber terbuka, serangan lapisan aplikasi, dan serangan jaringan.
2. Pentingnya Pembaruan dan Pemantauan Keamanan: Penelitian menunjukkan bahwa pembaruan perangkat lunak secara teratur dan pemantauan keamanan kontinu adalah kunci dalam menjaga keamanan aplikasi seluler. Kerentanannya bisa muncul setelah aplikasi diluncurkan, dan pembaruan rutin diperlukan untuk mengatasi celah keamanan yang mungkin baru muncul.
3. Pentingnya Pelatihan dan Kesadaran: Pengguna aplikasi seluler juga harus memahami praktik keamanan dan berperan dalam melindungi data pribadi mereka. Penelitian menunjukkan bahwa pelatihan dan peningkatan kesadaran tentang ancaman keamanan dapat membantu mengurangi risiko.

UCAPAN TERIMAKASIH

Penelitian ini merupakan hasil kolaborasi dosen dan mahasiswa yang dikemas dalam program Kuliah Kerja Nyata mahasiswa Unuversitas Nurul Jadid Paiton Probobolinggo Dalam program Kuliah Kerja Nyata ini ada banyak manfaat yang dapat diambil baik oleh pihak Unuja, pihak dosen maupun pihak mahasiswa. Luaran dari program ini adalah sebagai bukti bahwa seluruh dosen Unuja aktif dalam melakukan tri dharma perguruan tinggi. Dalam melakukan penelitian dan pengabdian dosen telah banyak dibantu oleh masiswa

sedangkan mahasiswa sejak dini telah dibimbing untuk melakukan penelitian serta bagaimana berinteraksi langsung dengan masyarakan dalam bentuk pengabdian. Syukur Alhamdulillah kami ucapkan atas kemudahan dan dukungan yang telah diberikan oleh pihak Unuja, mahasiswa, rekan-rekan dosen serta pihak LP3M yang telah banyak membantu atas suksesnya program ini.

REFERENSI

[1.] Aziz Alimul Hidayat, Studi Kasus Keperawatan; Pendekatan Kualitatif, Hidayat,Health Books Publishing, 2021

[2.] Bimo Walgito, Bimbingan dan Konseling (Studi & Kasus). Yogyakarta: Andi ,2010.

[3.] Fiqqih Anugerah, Tantimin, Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi, 2022.

[4.] Ikhsan Radiansyah, Candiwan, Yudi Priyadi, Analisis Ancaman Phishing Dalam Layanan Online Banking, 2016.

[5.] Mohd. Yusuf DM, Addermi, Jasmine Lim,. Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia.2022.

[6.] Muh. Amirul Mu'min, Abdul Fadlil , Imam Riadi, Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework, 2022.

[7.] Mesra Betty Yel, Mahyuddin K.M. Nasution, Keamanan Informasi Data Pribadi Pada Media Sosial, JIK, 2022.

[8.] Nunu Vadila, Ahmad R. Pratama, Analisis Kesadaran Keamanan Terhadap Ancaman Phising, 2021.

[9.] Rahardjo, Susilo dan Gudnanto, Pemahaman Individu Tekhnik Non Tes.Kudus: Nora Media Enterprise, 2011.

[10.] Ririn Aswandi, Putri Rofifah Nabilah Muchsin,Muhammad Sultan, Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS), LEGALITAS, 2020.

[11.] Tony Dwi Susanto Metode Penelitian Studi Kasus, ITS, (2020)

[12.] Wahyuningsih, Sri, Metode penelitian studi kasus. Madura: UTM Press, 2013.

[13.] Zuhri Halim, Prediksi Website Pemancing Informasi Penting Phising Menggunakan Support Vector Machine (SVM), 2017