CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 1, Mei 2020, hlm. 14-19

EVALUASI KEAMANAN INFORMASI *E-GOVERNMENT* MENGGUNAKAN MODEL *DEFENSE IN DEPTH*

Fanny Novianto

Program Studi Informatika
Fakultas Sains dan Teknologi, UIN Sunan Kalijaga
Email : fannynovianto@yahoo.co.id

Abstrak

Kemajuan Teknologi Informasi dan Komunikasi (TIK) yang demikian pesat memudahkan masyarakat dalam berkomunikasi dan mendapatkan informasi. Informasi yang bernilai strategis perlu dilakukan pengamanan dan pemangku kepentingan harus menyadari segala potensi kerawanan dalam transaksi sistem informasi dan komunikasi. Terdapat beberapa aspek yang harus dipenuhi dalam membangun keamanan sistem informasi dalam *e-government*. Aspek pertama yang harus dipenuhi adalah *confidentially* dan *privacy*. Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia saat ini menerapkan e-*government* dalam proses bisnis internal dan layanan publik. Salah satunya adalah penggunaan Sistem Database Pemasyarakatan (SDP). Data dan informasi dalam SDP bersifat rahasia karena salah satunya memuat tentang data dan informasi pelaku kriminal di Indonesia. Dengan pemanfaatan teknologi informasi dan semakin banyaknya informasi yang disajikan oleh pemerintah sebagai bagian dari pelayanan publik semakin besar pula kerentanan terhadap keamanan dan kerahasiaan sistem informasi itu sendiri. Metode penelitian yang digunakan adalah metode kualitatif dengan pendekatan studi kasus dengan penerapan model *defense in depth* untuk menganalisa keamanan informasi yang melibatkan beberapa lapisan keamanan untuk menjaga informasi agar tetap aman. Hasil analisa deskriptif menjelaskan bahwa perancangan dan pengembangan SDP memperhatikan prinsip dasar keamanan informasi yaitu kerahasiaan, integritas dan ketersediaan data. Namun terdapat kerentanan celah keamanan informasi yang sangat mungkin terjadi pada lapisan *host defense*, *network defense*, dan *physical defense*.

Kata kunci: *keamanan informasi, e-government, SDP, defense in depth*

EVALUATION OF E-GOVERNMENT INFORMATION SECURITY USING THE DEFENSE IN DEPTH MODEL

Abstract

The rapid progress of Information and Communication Technology (ICT) makes it easier for people to communicate and get information. Information of strategic value needs to be safeguarded and stakeholders must be aware of all potential vulnerabilities in information and communication system transactions. There are several aspects that must be met in building information security in e-government. The first aspect that must be met is confidentially and privacy. The Ministry of Law and Human Rights of the Republic of Indonesia is currently implementing e-government in internal business processes and public services. One of them is the use of the Correctional Database System (SDP). Data and information in SDP are confidential because one of them contains data and information on criminal offenders in Indonesia. With the use of information technology and the more information presented by the government as part of public services the greater the vulnerability to the security and confidentiality of the information system itself. The research method used is a qualitative method with a case study approach with the application of the defense in depth model to analyze information security involving several layers of security to keep information safe. Descriptive analysis results explain that the design and development of SDPs pay attention to the basic principles of information security, namely confidentiality, integrity and availability of data. But there are vulnerabilities in information security loopholes that are very likely to occur at the layer of host defense, network defense, and physical defense.

Keywords: *information security, e-government, SDP, defense in depth*

1. PENDAHULUAN

Kemajuan Teknologi Informasi dan Komunikasi (TIK) yang demikian pesat memudahkan masyarakat dalam berkomunikasi dan mendapatkan informasi. Informasi yang bernilai strategis perlu diperlakukan secara khusus, dan oleh karena itu semua pihak terutama para pemangku kebijakan harus mengerti arti pentingnya pengamanan informasi dan menyadari segala potensi kerawanan dalam transaksi sistem informasi dan komunikasi.

Ada enam strategi yang harus dilakukan dalam pengembangan *e-government*, strategi pertama mengembangkan sistem pelayanan yang handal dan terpercaya, serta terjangkau oleh masyarakat luas. Kedua menata sistem dan proses kerja pemerintah dan pemerintah daerah otonom secara holistik. Strategi ketiga yaitu memanfaatkan teknologi informasi dan komunikasi secara optimal. Strategi keempat adalah meningkatkan peran serta dunia usaha dan mengembangkan industri telekomunikasi dan teknologi informasi dalam negeri. Strategi kelima adalah meningkatkan kapasitas sumber daya manusia disertai dengan meningkatkan elektronifikasi masyarakat, dan strategi keenam adalah melaksanakan pengembangan secara sistematis melalui tahapan yang realistik dan terukur (Presiden RI 2003).

Dalam penerapan *e-government*, terdapat beberapa resiko atau kerawanan di dalamnya, antara lain resiko kecurangan, kesalahan, keterlambatan, interupsi layanan dan *safety critical system*. Kerawanan sistem *e-government* dapat diturunkan tingkatnya dengan cara mengintegrasikan aspek layanan keamanan informasi dan *security control* yang bersifat prosedural maupun administratif.

Terdapat beberapa aspek yang harus dipenuhi dalam membangun keamanan sistem informasi dalam *e-government*. Aspek pertama yang harus dipenuhi adalah *confidentially* dan *privacy*, hal ini diperlukan untuk menjaga informasi dari orang yang tidak berhak mengakses. Untuk meningkatkan jaminan *privacy* dapat menggunakan *kriptografi* dan *steganografi*. Aspek kedua adalah *integrity* dimana dalam aspek ini informasi maupun sistem tidak boleh diubah tanpa seijin pemilik informasi. Aspek ketiga adalah *availability* yaitu ketika dibutuhkan, pengguna yang berhak akan selalu dapat mengakses informasi dan aset yang berkaitan. Untuk aspek keempat dan kelima adalah *authentication* dan *access control*. Sedangkan aspek *non repudiation* adalah aspek keenam yang harus dipenuhi. Dalam aspek ini seseorang tidak dapat menyangkal bahwa ia telah mengirimkan suatu data digital (Richardus, Indrajit, and Eko 2011).

Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia saat ini menerapkan e-*government* dalam proses bisnis internal dan layanan publik. Berbagai inovasi telah dilakukan oleh Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia untuk mengembangkan *e-government* yang ditujukan untuk melayani masyarakat, menghilangkan pungutan liar dan menciptakan kinerja yang transparan dan akuntabel. Salah satunya adalah penggunaan Sistem Database Pemasyarakatan (SDP).

SDP adalah solusi teknologi informasi yang komprehensif yang mencakup semua proses bisnis Pemasyarakatan. SDP didefinisikan sebagai seluruh sistem informasi yang meliputi pengumpulan, penyaringan, manajemen, presentasi dan komunikasi informasi Pemasyarakatan. Tujuan pengembangan SDP adalah untuk memberikan informasi pemasyarakatan sebagai upaya untuk meningkatkan layanan publik kepada lembaga pemerintah, masyarakat dan Warga Binaan Pemasyarakatan (WBP) yang efektif, efisien, akuntabel, dan transparan melalui teknologi informasi.

Data dan informasi dalam SDP bersifat rahasia karena salah satunya memuat tentang data dan informasi pelaku kriminal di Indonesia (Kemenkumham 2016). Hanya data dan informasi tertentu atas persetujuan Menteri Hukum dan Hak Asasi Manusia Republik Indonesia yang diijinkan untuk di bagi kepada masyarakat. Dengan pemanfaatan teknologi informasi dan semakin banyaknya informasi yang disajikan oleh pemerintah sebagai bagian dari pelayanan publik semakin besar pula kerentanan terhadap keamanan dan kerahasiaan sistem informasi itu sendiri (A. Wijaya 2019).

Ruang lingkup dalam penelitian ini adalah penerapan e-*government* SDP di lingkungan Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia. Metode penelitian yang digunakan adalah penerapan model *defense in depth* untuk menganalisa keamanan informasi yang melibatkan beberapa lapisan keamanan untuk menjaga informasi agar tetap aman.

2. TINJAUAN PUSTAKA

2.1 *e-government*

e-government bukanlah sebuah obat atau jalan pintas menuju pada perbaikan atau pertumbuhan ekonomi yang signifikan secara cepat, atau pencapaian efisiensi kinerja pemerintahan dalam waktu singkat, atau pembentukan mekanisme pemerintahan yang bersih dan transparan; *e-government* adalah sarana atau alat untuk menuju kepada obyektif-obyektif tersebut (R. E. Indrajit, A. Zainuddin, and D. Rudianto 2007) **.**

Penerapan *e-government* merupakan bentuk dari implementasi penggunaan teknologi informasi bagi pelayanan pemerintah kepada publik yaitu bagaimana pemerintah memberikan informasi kepada pemangku kepentingan (*stakeholder*) melalui sebuah portal web. Alasan utama mengimplementasikan e-government (E. Indrayani 2016) .

a. *e-government* meningkatkan efisiensi;
b. *e-government* memperbaiki kualitas pelayanan;

c. *e-government* membantu mencapai keluaran kebijakan yang lebih baik;
d. *e-government* berkontribuusi dalam mencapai tujuan ekonomi;
e. *e-government* dapat menjadi kontributor utama dalam pelaksanaan reformasi;
f. *e-government* membangun kepercayaan antara pemerintah dan warga negara/*citizens*.

2.2 Keamanan Informasi

Informasi merupakan aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu maka perlindungan terhadap informasi (keamanan informasi) merupakan hal yang mutlak harus diperhatikan secara sungguh-sungguh oleh segenap jajaran pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi.

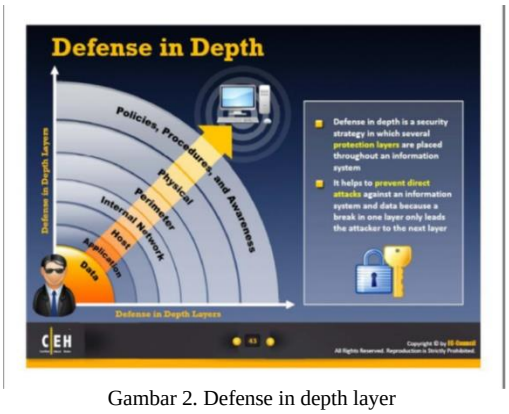
Prinsip Keamanan adalah sebagai berikut (H. Azaim 2017) :

a. Kerahasiaan : memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya;
b. Integritas : melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif;
c. Ketersediaan : memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Gambar 1. Prinsip keamanan informasi

2.3 *Defense In Depth*

Sebuah konsep dalam keamanan teknologi informasi yang melibatkan beberapa lapisan keamanan untuk menjaga informasi agar tetap aman. Ide dibalik pendekatan Defense in Depth adalah untuk mempertahankan sistem terhadap serangan tertentu dengan menggunakan beberapa metode independen. Konsep ini digagas oleh National Security Agency (NSA) sebagai pendekatan komprehensif untuk keamanan informasi (T. Hendra 2017).Tujuannya adalah untuk meningkatkan biaya dan usaha serangan terhadap sistem TI yang dimiliki sebuah organisasi dengan mendeteksi serangan, melakukan respon terhadap serangan dan menyediakan lapisan pertahanan.



Gambar 2. Defense in depth layer

1. *Layer 1 : Data Defense*
   Data adalah salah satu sumber daya paling berharga di banyak organisasi. Jika data menjadi rusak, hilang atau terexpose pesaing maka banyak organisasi akan terpengaruh. Data dapat dilindungi melalui penggunaan Daftar kontrol akses (ACLs) pada file dan folder, enkripsi dan strategi backup and restore yang efektif;
2. *Layer 2 : Application Defense*
   Lapisan keamanan aplikasi mengontrol akses ke informasi sensitif. Ini termasuk server web, *e-commerce*, layanan internet dan suara. Aplikasi dapat dilindungi melalui penggunaan otentikasi, otorisasi dan kebijakan password;
3. *Layer 3 : Host Defence*
   Host merupakan komputer yang menjalankan aplikasi klien dan server.
4. *Layer 4 : Network Defense*
   Segmen jaringan terdiri dari dua atau lebih perangkat yang berkomunikasi satu sama lain pada bagian jaringan fisik atau logis yang sama. Jika segmennya logis, mereka disebut sebagai virtual local area networks (VLAN). Pengguna domain tidak boleh diberi akses administrator lokal untuk menghindari penghapusan atau penginstalan perangkat lunak yang tidak diinginkan;
5. *Layer 5 : Perimeter Defense*
   Jaringan ditambahkan antara jaringan yang dilindungi dan jaringan eksternal untuk memberikan lapisan keamanan tambahan. Setiap layanan yang diberikan kepada pengguna di jaringan eksternal dapat ditempatkan di perimeter jaringan;
6. *Layer 6 : Physical Defense*
   Akses fisik ke komputer akan memberi pencuri data kesempatan untuk menonaktifkan kata sandi.Server yang harus dijaga adalah lingkungan yang aman dimana hanya personil tertentu yang memiliki akses;
7. *Layer 7 : Policies, Procedures, dan Awareness*
   Prinsip-prinsip keseluruhan mengatur strategi keamanan dari organisasi manapun. Tanpa

lapisan ini, seluruh strategi gagal. Kebijakan dan praktik keamanan tertulis dengan baik.

3. METODOLOGI PENELITIAN

Dalam penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus yang merupakan metode analisis deskriptif terfokus pada suatu aktivitas tertentu untuk diamati dan dianalisis secara cermat hingga tuntas.

Teknik pengumpulan data yang digunakan melalui wawancara, observasi dan studi literatur. Dalam wawancara, narasumber yang dipilih adalah yang berkaitan langsung dengan SDP sesuai level dalam SDP yaitu operator, supervisor dan administrator. Dalam observasi dilakukan pengamatan secara langsung aktivitas dalam SDP muai dari level operator hingga administrator. Studi literatur digunakan dengan mempelajari peraturan-peraturan, kebijakan, dokumen standar operasional prosedur dan dokumen pendukung lainnya yang relevan dengan penelitian.

Tahapan penelitian yang digunakan adalah sebagai berikut :

1. Menentukan objek penelitian yaitu Sistem Database Pemasyarakatan Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia;
2. Melakukan studi literatur untuk mengumpulkan informasi tentang teori, konsep, metode yang relevan;
3. Mengidentifikasi dan mendeskripsikan *defense in depth layer*;
4. Pengumpulan data melalui observasi dan wawancara;
5. Pengolahan data yang telah dikumpulkan sesuai dengan *layer* yang ditentukan;
6. Melakukan analisa deskriptif dari data yang telah diolah sesuai dengan *layer*;
7. Memberikan kesimpulan berdasarkan *defense in depth layer*.

4. HASIL DAN PEMBAHASAN

Hasil analisa *defense in depth layer* terhadap penerapan SDP di Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia adalah sebagai berikut :

1. *Layer 1 : Data Defense*

Pengamanan data dalam SDP dilakukan dengan cara memberikan *access control* dimana user diberikan hak akses tertentu untuk mengakses sistem atau informasi. Administrator SDP mengamankan informasi dengan cara mengatur hak atas informasi apa saja yang boleh diakses oleh operator dan supervisor. Hak akses meliputi hanya melihat, hak akses penuh, tidak punya akses, dual password dan hak delete. Fitur dual password digunakan apabila memerlukan akses ke fitur tertentu dan membutuhkan izin dari supervisor.

Fitur tambahan untuk pengamanan data dengan menggunakan fungsi log file yang menginformasikan waktu, jenis file, nama user yang melakukan perubahan dan log pengguna yang memberikan informasi nama user, waktu, jenis perubahan dan info akses aplikasi. Strategi *backup* dan *restore* data dilakukan secara efektif dimana proses backup data dilakukan rutin secara harian dan berjalan otomatis

Dalam SDP juga memungkinkan pertukaran data antar instansi penegak hukum lainnya yakni Kepolisian, Kejaksaan dan Mahkamah Agung. Proses pertukaran data dan informasi antar instansi melalui proses enkripsi yang diamankan dalam Otorisasi Sertifikat Digital (OSD) oleh Lembaga Sandi Negara (Kemkominfo 2016).

2. *Layer 2 : Application Defense*

Di level pengamanan aplikasi, manajemen password pada awalnya di tentukan oleh administrator kepada operator dan supervisor dan berikutnya dilakukan penggantian password oleh masing-masing operator dan supervisor. Ancaman utama yang terjadi adalah terkait *security awareness* dimana operator/supervisor dengan mudah memberikan password ke orang yang dikenal.

Sistem otentikasi sudah tersedia melalui sertifikat digital yang menjamin keabsahan informasi. Tidak hanya itu, fitur *biometric* menggunakan sidik jari sudah tersedia khusus pemberian layanan informasi bagi WBP sehingga tidak mungkin ada penyalahgunaan informasi. Untuk sistem otorisasi sudah dilakukan pada user dengan tingkatan yang berbeda untuk mengakses informasi tertentu.

Patch Management sudah dilakukan dengan tujuan untuk memperbaiki program, meningkatkan fitur aplikasi dan menambal celah keamanan (*vulnerabilities*) yang ditemukan (H. Bintara 2017). Dalam *patch management*, administrator akan menerima notifikasi yang berisi ketersediaan *patching*,berikutnya vendor akan menginformasikan *patch scheduling* kepada administrator untuk melakukan *download* dan *update patch*. Dalam proses *patch deployment* dan *post deployment* dilakukan pengawasan oleh vendor untuk memastikan proses berjalan dengan baik.

3. *Layer 3 : Host Defence*

Sistem operasi pada host yang menjalankan aplikasi SDP pada server dan klien menggunakan Windows Server 2012. Sistem operasi ini memiliki cakupan keamanan yang cukup baik dibandingkan Windows versi sebelumnya. Akan tetapi ancaman terhadap sistem operasi pada host tetap memungkinkan. Administrator tidak melakukan *operating system hardening* yaitu proses untuk menilai atau menimbang apakah arsitektur keamanan pada sistem operasi berjalan baik atau tidak, tidak dilakukan *audit policy* untuk mengantisipasi berbagai serangan terhadap sistem operasi(Fahmi 2014).

Perangkat lunak anti virus yang terinstall tidak *up to date* dan menggunakan perangkat lunak dengan kemampuan terbatas atau free antivirus. Celah keamanan lainnya adalah perangkat lunak, services atau package yang tidak perlu terinstall pada sistem operasi. Idealnya semua perangkat lunak, services atau packages yang tidak diperlukan oleh sistem operasi dihilangkan dan cukup menggunakan services standar pada sistem operasi sebelum terhubung dengan internet.

4. *Layer 4 : Network Defense*

Jalur komunikasi yang digunakan dalam SDP terenkripsi dengan Virtual Private Network (VPN) melalui aplikasi Logmein Hamachi. Dengan aplikasi ini antara server dengan klien atau antar komputer terhubung secara langsung melalui internet secara private dan untuk mengakses network VPN melalui proses otentikasi dan enkripsi.

Proses pengaman jaringan yang digunakan pada SDP terbatas pada penggunaan VPN. Lemahnya pengamanan fisik jaringan menimbulkan kerentanan keamanan informasi.

5. *Layer 5 : Perimeter Defense*

Penerapan perimeter defense dilakukan dengan menggunakan router mikrotik, akan tetapi hanya terbatas pada konfigurasi standar mikrotik seperti penggantian username dan password router mikrotik. Belum ada upaya untuk mengoptimalkan penggunaan mikrotik sebagai *perimeter defense*.

Untuk optimalisasi keamanan jaringan bisa dengan menerapkan Demilitarized Zone (DMZ) dengan tujuan untuk menambahkan lapisan keamanan jaringan area lokal (LAN)(L. Cleghorn 2013). Dengan menggunakan DMZ, dari jaringan publik, untuk bisa mengaksesnya, peran router yang terkoneksi sangat dibutuhkan. DMZ sangat berguna sebagai keamanan, karena jaringan publik tidak langsung terkoneksi dengan server.

6. *Layer 6 : Physical Defense*

Upaya pembatasan akses fisik ke server sudah dilakukan dengan menempatkan pada ruangan khusus dan akses terbatas hanya pada administrator. Server ditempatkan pada lokasi yang aman dari banjir dilengkapi pendingin udara (AC) dan *fire security system*.

Kerentanan terletak pada penempatan perangkat jaringan yang mudah di akses oleh siapapun. Kabel-kabel yang tidak dikelola secara rapi menimbulkan ancaman yang cukup serius dan menyulitkan prosedur perbaikan ketika terjadi masalah pada jaringan.

7. *Layer 7 : Policies, Procedures, dan Awareness*

Sumber daya manusia adalah yang terlemah dalam sebuah rantai pengamanan. Upaya yang dilakukan untuk mengoptimalkan keamanan informasi dari sisi sumber daya manusia antara lain melalui menetapkan peraturan-peraturan dan sanksi terhadap pelanggaran berupa Peraturan Menteri Hukum dan HAM Republik Indonesia, menerapkan sistem operasional prosedur untuk mengefektifkan proses, meningkatkan kepedulian user terhadap keamanan informasi melalui pelatihan-pelatihan.

5. KESIMPULAN

Berdasarkan uraian dari hasil dan pembahasan, dapat diambil kesimpulan sebagai berikut :

1. Perancangan dan pengembangan SDP memperhatikan prinsip dasar keamanan informasi yaitu kerahasiaan, integritas dan ketersediaan data.
2. Data dan informasi dalam SDP bersifat rahasia, dalam pengembangan SDP untuk menjaga kerahasiaan data diberlakukan akses terbatas sesuai dengan hak dan kewenangan, lalu lintas user dalam penggunaan SDP terekam dalam log file dan log pengguna. Untuk menjaga integritas data dalam SDP, Kementerian Hukum dan HAM bekerjasama dengan Lembaga Sandi Negara yang mengeluarkan Otorisasi Sertifikat Digital (OSD) yang menjamin otentikasi informasi ketika dilakukan pertukaran data dan informasi antar nstansi penegak hukum;
3. Untuk menjamin ketersediaan data sudah dilakukan prosedur backup data secara harian, apabila terjadi kehilangan data bisa segera dilakukan restore data;
4. Prosedur pengamanan aplikasi dilakukan dengan cara menggunakan *password strength* dari administrator kepada user operator/supervisor, penggunaan fitur *biometric* menggunakan sidik jari WBP dan *patching* untuk memperbaiki program dan menambal celah keamanan.
5. Kerentanan celah keamanan informasi sangat mungkin terjadi pada lapisan *host defense*, *network defense*, dan *physical defense*.
6. Instalasi antivirus yang tidak *up to date*, penggunaan perangkat lunak *free edition* dengan kemampuan terbatas, instalasi services atau packages yang tidak dibutuhkan pada host server, lemahnya pengamanan fisik jaringan dan kurangnya *security awareness* dari sumber daya manusia merupakan titik kerentanan keamanan informasi.

DAFTAR PUSTAKA

A. WIJAYA. 2019. “Information Security Strategy To Counter Cyber Threats in Electronic Procurement Systems”. *Study of Hacker Attacks* 5: 71–86.

E. INDRAYANI. 2016. *E-Government : Konsep, Implementasi Dan Perkembangan Di Indonesia*.

FAHMI. 2014. “Mengenal System Hardening (FreeBSD System)”. July 4, 2014 <https://www.fahmi.my.id/mengenal-

system-hardening.html> [accessed 5 May 2020].

H. AZAIM. 2017. “Mengenal Confidentiality, Integrity, Dan Availability Pada Keamanan Informasi”. Netsec Indonesia. January 5, 2017 <https://netsec.id/confidentiality-integrity-availability-keamanan-informasi/> [accessed 3 May 2020].

H. BINTARA. 2017. “Pentingnya Patch Management”. Netsec Indonesia. February 1, 2017 <https://netsec.id/pentingnya-patch-management/> [accessed 2 December 2019].

KEMENKUMHAM. 2016. “P. M. H. Dan H. A. M. R. I. Nomor 39 Tahun 2016, ‘Sistem Database Pemasyarakatan,’”.

KEMKOMINFO. 2016. “P. M. K. Dan I. R. I. No. 4 Tahun 2016, ‘Sistem Manajemen Pengamanan Informasi’”.

L. CLEGHORN. 2013. “Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth”. *Journal of Information Security* 04: 144–49. <https://doi.org/10.4236/jis.2013.43017>.

PRESIDEN RI. 2003. “Instruksi Presiden RI No.3 Tahun 2003, ‘Kebijakan Dan Strategi Nasional Pengembangan E-Government,’”.

R. E. INDRAJIT, A. ZAINUDDIN AND D. RUDIANTO. 2007. *Electronic Government in Action. 2007*.

RICHARDUS, INDRAJIT AND EKO. 2011. *Manajemen Keamanan Informasi Dan Internet*.

T. HENDRA. 2017. “Denfense in Depth”. June 8, 2017 <https://medium.com/@tonyhendrap/denfense-in-depth-6e3928899b10> [accessed 29 April 2020].