Jurnal Teknologi Informasi dan Komunikasi
Vol: 14 No 01 2023 **E-ISSN: 2477-3255**
Diterima Redaksi: 18-04-2023 | Revisi: 30-04-2023 | Diterbitkan: 26-05-2023

Ransomware Attacks Threat Modeling Using Bayesian Network

Sulistiadi[1], Muhammad Salman[2]
[1,2]Program Studi Teknik Elektro – Fakultas Teknik Universitas Indonesia
[1,2]Kampus Universitas Indonesia, Depok, Jawa Barat 16424, Indonesia
E-mail: [1]sulistiadi@ui.ac.id, [2]muhammad.salman@ui.ac.id

Abstract

Ransomware is a dangerous malware that blocks access to data through encryption, and it exploits device vulnerabilities to perform chain attacks from one system to another. This study results in modeling the threat of ransomware attacks using Bayesian Network. The structure of the model is created using device vulnerabilities that can be exploited. As the basis for calculating the probability of the model, the EPSS vulnerability score is used. The risk exposure rating is calculated through the joint probability distribution formulation based on attack scenarios. Our model shows that ransomware attacks are most likely to exploit the chain of vulnerabilities CVE-2021-26855, CVE-2021-26857, CVE-2021-27065, CVE-2021-36942, and CVE-2017-0144 which has a probability value of 0.046534. In addition, the use of the EPSS also makes the risk assessment more factual, accurate, and effective. The threat modeling method can help in identifying ransomware attacks through a chain of vulnerabilities, making risk assessment more precise.

Keywords: *Ransomware, Risk Assessment, Threat Modeling, Bayesian Network, EPSS*

Pemodelan Ancaman Serangan *Ransomware* Menggunakan Bayesian Network

Abstrak

Ransomware merupakan salah satu bentuk malware berbahaya karena serangannya yang memblokir hak akses ke data melalui enkripsi. Serangan ransomware memanfaatkan kerentanan-kerentanan pada perangkat sehingga membentuk serangan berantai dari suatu sistem ke sistem lainnya. Penelitian ini menghasilkan pemodelan ancaman serangan ransomware menggunakan Bayesian Network. Pemodelan ancaman disusun menggunakan celah-celah kerentanan yang dapat dieksploitasi oleh penyerang dalam melancarkan serangan ransomware. Sebagai dasar perhitungan probabilitas pada model, digunakan skor kerentanan EPSS. Penilaian paparan risiko dihitung melalui formulasi distribusi probabilitas gabungan berdasarkan skenario serangan. Dari pemodelan yang terbentuk, serangan ransomware melalui eskploitasi rantai kerentanan CVE-2021-26855, CVE-2021-26857, CVE-2021-27065, CVE-2021-36942, dan CVE-2017-0144 menjadi jalur serangan yang probabilitasnya tertinggi, sebesar 0.046534. Selain itu, penggunaan skor EPSS pada penelitian ini juga membuat

penilaian risiko lebih faktual, akurat, dan efektif. Melalui metode pemodelan ancaman yang dihasilkan, serangan ransomware yang dilakukan melalui rantai kerentanan dapat lebih mudah diidentifikasi sehingga penilaian risiko menjadi lebih tepat.

Kata kunci: *Ransomware, Penilaian Risiko, Pemodelan Ancaman, Bayesian Network, EPSS*

1. Pendahuluan

Dalam beberapa tahun terakhir, *ransomware* telah menjadi salah satu ancaman terbesar bagi keamanan siber dunia. Pada tahun 2022, Badan Siber dan Sandi Negara menyatakan bahwa terdapat 17 serangan *ransomware* ke berbagai organisasi di Indonesia [1]. Terjadi kenaikan jumlah serangan apabila dipadankan dengan tahun 2021 yang hanya sebesar 15 serangan. Banyak faktor yang menyebabkan serangan semakin meningkat, salah satunya adalah potensi keuntungan yang besar. *Ransomware* merupakan bentuk *malware* yang menghilangkan akses yang sah ke data pengguna melalui teknik enkripsi. Setelah data terenkripsi, dibutuhkan kunci dekripsi untuk kembali membuka akses ke data tersebut. Untuk memberikan kunci dekripsi tersebut, penyerang meminta tebusan sejumlah uang dengan nominal tertentu dalam mata uang digital [2]. Korban *ransomware* menginginkan kembali data berharga mereka, dan mereka membayar uang tebusan untuk mendapatkan kunci dekripsi dari penyerang. Hal inilah yang menyebabkan serangan *ransomware* mempunyai keuntungan ekonomi yang besar bagi para penyerang.

Ransomware tidak hanya menyerang target perseorangan. Pada skala yang besar, *ransomware* juga menyerang organisasi bisnis, kesehatan, dan pemerintahan. Misalnya, pada Mei 2017 terdapat lebih dari 300.000 komputer di sekitar 150 negara yang terinfeksi serangan *ransomware* [3]. Pada serangan yang lain, varian *ransomware* NotPetya yang menargetkan bisnis dan institusi pemerintah Ukraina. Tidak hanya di Ukraina, NotPetya juga berhasil menyerang perusahaan global dunia, termasuk Merck, TNT Express, Saint-Gobain, Maersk, dan Mondelez [4]. Pada tahun 2019, varian *ransomware* lainnya, Conti, berhasil menyerang layanan kesehatan dan lembaga peradilan di Amerika Serikat, serta lebih dari 400 organisasi di seluruh dunia [5]. Salah satu yang terdampak Conti adalah vendor penyimpanan cadangan ExaGrid yang membayar tebusan sebesar $2,6 juta pada penyerang [6].

Terdapat beberapa cara yang dijadikan vektor serangan dalam *ransomware*. National Cyber Security Centre (NCSC) Kerajaan Inggris menyatakan bahwa terdapat tiga vektor serangan yang umumnya digunakan oleh *ransomware*, yaitu Remote Desktop Protocol (RDP), *phishing* pada *email*, dan celah kerentanan perangkat [7]. Vektor pertama, yaitu RDP, memungkinkan seseorang untuk mengakses komputer dari jarak jauh. Metode *brute-force* terhadap akun pengguna dan kata sandi sering digunakan untuk mendapatkan akses awal ke komputer korban. Kemudian, selama sesi RDP, penyerang menggunakan fungsi *clipboard* dan *shared folder* untuk melakukan instalasi *ransomware* di komputer tersebut [8]. Vektor kedua, penyerang memanfaatkan *email* untuk mengirim *email* yang terlihat asli, seringkali dengan subjek atau lampiran yang menarik perhatian penerima, namun sebenarnya berisi *file* yang mengandung *ransomware* [9]. Ketika pengguna membuka lampiran atau mengikuti tautan dalam *email* tersebut, *ransomware* akan diunduh dan mulai menyebar di komputer korban dan jaringan perusahaan. Vektor terakhir, melalui celah kerentanan perangkat yang ditemukan oleh penyerang. Jika sebuah perangkat atau sistem tidak diperbarui dengan *patch* keamanan terbaru, celah keamanan tersebut dapat dimanfaatkan untuk menyebarkan *ransomware* pada komputer atau jaringan melalui Exploit Kits [10].

Isu *ransomware* merupakan bentuk risiko yang harus dikendalikan oleh organisasi agar tidak timbul kerugian secara legal, finansial, dan reputasi. Risiko dalam organisasi dapat dikendalikan dengan cara melakukan asesmen risiko. Dalam proses asesmen risiko terdapat komponen pemodelan ancaman yang dapat mengidentifikasi dan menilai seberapa besar kemungkinan ancaman yang dapat menyerang organisasi. Akan tetapi, pemodelan ancaman pada umumnya hanya berfokus pada variabel aset, sistem, frekuensi serangan, dan jumlah

https://doi.org/10.31849/digitalzone.v14i1. 13788

kerentanan yang berbeda dan independen.Dalam dunia nyata, serangan siber dilakukan secara terstruktur dan sistematis. Serangan dilakukan melalui beberapa aktivitas yang dieksekusi secara bertahap. Penyerang seringkali memanfaatkan rantai celah kerentanan perangkat yang dimiliki oleh organisasi. Antara satu serangan dengan serangan lainnya dapat memiliki hubungan kausalitas sehingga memiliki ketergantungan satu sama lain. Misalnya, *ransomware* DearCry yang memanfaatkan beberapa celah kerentanan pada Microsoft Exchange, yaitu CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, dan CVE-2021-27065 [11]. Penyerang melakukan serangan berantai dengan mengeksploitasi kerentanan-kerentanan tersebut sampai dengan berhasil melakukan instalasi *ransomware* di sistem target. Dengan kondisi tersebut, serangan dapat mengeksploitasi rantai kerentanan terkait untuk menyerang aset yang tidak terbatas jumlahnya. Apabila penilaian risiko dilakukan secara parsial dan independen, ancaman dari hasil eksploitasi rantai kerentanan tersebut tidak dapat teridentifikasi dengan baik dan peniliaian risiko pun menjadi tidak akurat.

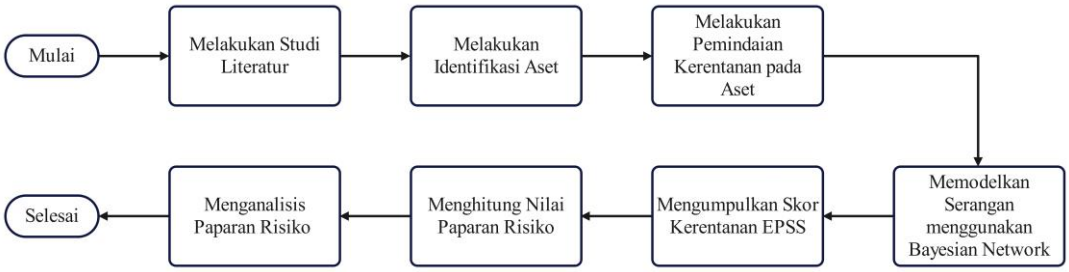
Dalam penelitian ini, dikembangkan pemodelan ancaman serangan *ransomware* yang menyerang melalui celah kerentanan. Pemodelan ancaman sendiri bukan hal yang baru dalam penilaian risiko. Sudah banyak standar pemodelan ancaman yang dibuat oleh para ahli seperti STRIDE, DREAD, dan OCTAVE Allegro. Standar tersebut banyak digunakan oleh penelitian terdahulu. Contohnya, STRIDE digunakan untuk mengidentifikasi dan memitigasi serangan *phishing* pada perangkat IoT [12]. Kemudian, STRIDE dan DREAD dikombinasikan pada penilaian risiko di ekosistem pasar digital [13]. Penelitian lainnya, OCTAVE Allegro dipakai untuk menilai risiko pada aset sistem teknologi informasi di sebuah institusi pendidikan [14]. Akan tetapi, penelitian-penelitian tersebut tidak memberikan pandangan menyeluruh pada kasus serangan siber yang dilakukan secara berantai karena memiliki kemampuan terbatas dalam menilai ketergantungan antara satu kerentanan dengan kerentanan lainnya yang dieksploitasi dalam serangan. Untuk menilai risiko pada serangan berantai, dalam penelitian ini digunakan pemodelan ancaman berbasis grafis dan statistik. Seperti yang dilakukan dalam penelitian yang menilai risiko pada sistem *e-learning* dengan menggunakan Petri Nets [15] dan penelitian yang menggunakan Bayesian Network untuk memodelkan serangan pada layanan *cloud* [16]. Dua penelitian tersebut memakai CVSS (Common Vulnerability Scoring System) untuk menilai tingkat keparahan kerentanan suatu perangkat. CVSS seringkali dipakai karena lebih memfokuskan penilaian pada karakteristik teknis kerentanan suatu perangkat. Namun demikian, CVSS tidak menggunakan data faktual dan terkini dalam memperhitungkan faktor probabilitas kemampuan penyerang dalam memanfaatkan kerentanan.

Dalam penelitian ini, dikembangkan metode baru dalam penilaian risiko pada serangan *ransomware* secara berantai melalui pemodelan Bayesian Network dengan menggunakan sistem penilaian EPSS (Exploit Prediction Scoring System). EPSS merupakan skor kerentanan perangkat yang menggunakan data faktual yang dapat memperikirakan seberapa besar kemungkinan suatu kerentanan perangkat akan dieksploitasi [17]. Penelitian ini setidaknya memberikan tiga kontribusi. Pertama, penelitian ini membuat pemodelan ancaman serangan berantai *ransomware* yang dapat menyebabkan terpaparnya aset organisasi menggunakan Bayesian Network. Kedua, memberikan gambaran penilaian tingkat probabilitas serangan berantai dengan memakai EPSS. Dua kontribusi tersebut dicapai dengan cara melakukan pemodelan ancaman serangan *ransomware* melalui eksploitasi beberapa celah kerentanan dari perangkat-perangkat yang dapat terpapar dari serangan *ransomware* DearCry. Kontribusi terakhir, penelitian ini mengevaluasi penilaian risiko yang telah dihasilkan dengan membuat tingkat prioritas dalam memperbaiki kerentanan perangkat. Dengan penelitian ini, organisasi dapat mencegah serangan siber yang menyerang melalui celah rantai kerentanan perangkat.

2. Metode Penelitian

Penelitian ini dilakukan dalam beberapa langkah seperti yang terdapat pada Gambar 1. Pertama, dilakukan studi literatur untuk memahami fase-fase serangan *ransomware* yang menjadi dasar penentuan metode pemodelan ancaman. Kedua, dilakukan identifikasi aset

sebagai objek penelitian ini, yaitu pada perangkat-perangkat di pusat data organisasi XYZ yang rentan terhadap serangan *ransomware*. Kemudian, dari aset yang berhasil teridentifikasi, dilakukan pemindaian celah kerentanan dengan memfokuskan pada kerentanan-kerentanan yang digunakan oleh *ransomware* DearCry pada serangan HAFNIUM. Setelah kerentanan teridentifikasi, disusun pemodelan serangan berantai *ransomware* ke model BN, lalu skor EPSS dari kerentanan tersebut dikumpulkan. Skor EPSS didapatkan melalui API EPSS pada URL https://api.first.org/data/v1/epss, sesuai dengan kondisi per 1 Maret 2023. Setelah, model BN terbentuk dan skor EPSS tersedia, dirumuskan formulasi penilaian risiko melalui penghitungan probabilitas serangan dan dilakukan penghitungan paparan risiko pada setiap fase serangan. Terakhir, dilakukan analisis hasil penghitungan tersebut dengan membandingkan nilai probabilitas setiap kemungkinan jalur serangan yang terbentuk dari celah kerentanan pada model. Jalur serangan yang memiliki probabilitas yang tinggi lebih rentan terpapar risiko serangan *ransomware* dibandingkan jalur serangan yang memiliki probabilitas yang rendah.



Gambar 1. Langkah-Langkah dalam Penelitian

2.1. Studi Literatur

2.1.1. Serangan *Ransomware* pada Celah Kerentanan

Berkaca pada teknik eksploitasi oleh *ransomware* DearCry, terdapat beberapa tahap yang dilakukan oleh penyerang untuk melakukan penyebaran *ransomware*. Gambar 2 mengilustrasikan rantai serangan tersebut. Pada fase awal serangan, penyerang berusaha untuk memasuki aplikasi melalui celah kerentanan yang berhubungan dengan sistem autentikasi. Melalui kerentanan tersebut, penyerang berekspektasi dapat melakukan penyusupan terhadap aplikasi tanpa melalui autentikasi. Setelah berhasil masuk ke dalam aplikasi, kemudian penyerang melakukan eskalasi hak akses di sistem operasi perangkat melalui RCE. Kemudian, penyerang dapat membuat sebuah *file* yang berisi kode berbahaya dengan memanfaatkan teknik RCE juga. Lalu, *file* berbahaya yang telah berhasil dibuat pada suatu perangkat dapat digunakan oleh penyerang untuk menyerang aset informasi/data pada perangkat tersebut. Pada level yang lebih berbahaya, penyerang dapat menggunakan *file* tersebut untuk memperluas serangan ke aset yang lebih kritikal seperti *server* yang berperan sebagai *domain controller*. Dengan menyerang ke *domain controller*, penyerang dapat menyembunyikan alat eksploitasi di perangkat lain [18] atau mengeksploitasi kerentanan EternalBlue SMB ke perangkat-perangkat yang bersistem operasi Windows [19]

2.1.2. Bayesian Network

Bayesian Network (BN) adalah model penggambaran probabilitas yang mewakili sekumpulan variabel. BN terdiri dari dua bagian, yaitu bagian kualitatif dan bagian kuantitatif. Bagian kualitatif menentukan ketergantungan bersyarat antara variabel yang direpresentasikan sebagai grafik, sedangkan bagian kuantitatif menunjukkan kekuatan dan sifat ketergantungan antar variabel yang direpresentasikan dalam Conditional Probability Table (CPT) [20].

BN diekspresikan sebagai diagram yang kompleks dan kausal, dengan melambangkan suatu biner $B = \langle G, \theta \rangle$, di mana:

- $G = (V, E)$ menunjukkan grafik asiklik terarah, di mana V adalah sekumpulan simpul yang menunjukkan variabel dalam domain masalah dan E adalah sekumpulan sisi yang menunjukkan ketergantungan kausal antar variabel.

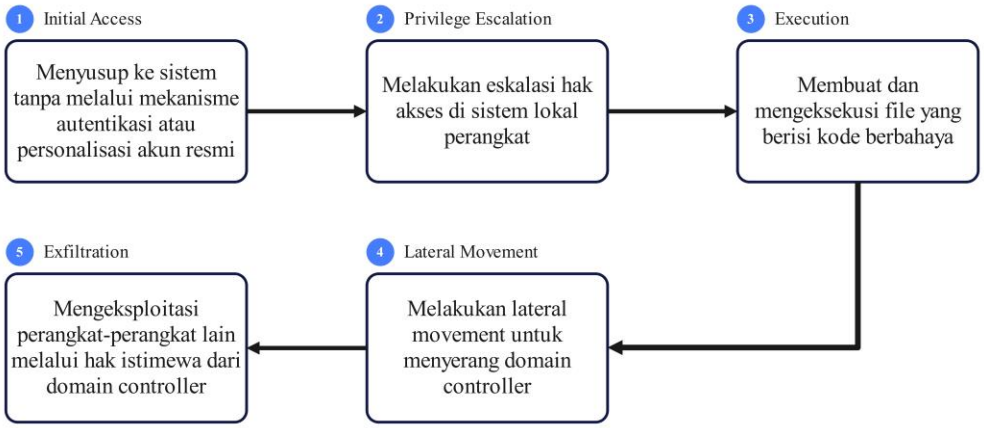
https://doi.org/10.31849/digitalzone.v14i1. 13788

- θ merupakan parameter jaringan termasuk probabilitas dalam CPT dari simpul-simpul BN. θ juga mengungkapkan tingkat pengaruh antara simpul dan mencerminkan fitur kuantitatif dalam suatu model.

BN juga dapat merepresentasikan distribusi probabilitas gabungan dari serangkaian variabel yang telah terkategorisasi. Berikut persamaan distribusi probabilitas gabungan serangkaian variabel dalam BN:

$$P(V_1, V_2, \dots, V_n) = \prod_{i=1}^{n} P\left(V_i \middle| Parents(V_i)\right) \quad (1)$$

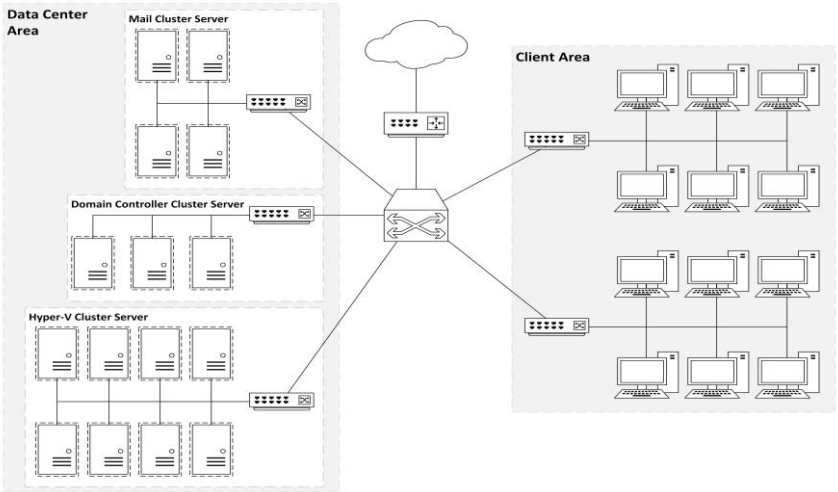
di mana $P(V_1, V_2, \dots, V_n)$ adalah distribusi probabilitas gabungan variabel tersebut, dan $Parents(V_i)$ menunjukkan simpul induk dari V_i.



Gambar 2. Rantai Serangan *Ransomware* melalui Beberapa Celah Kerentanan

2.2. Identifikasi Aset dan Kerentanan

Pada tahap ini, dilakukan identifikasi aset dari pusat data *on-premise* yang ada di organisasi XYZ. Gambar 3 mengilustrasikan topologi infrastruktur pusat data organisasi XYZ. Topologi tersebut terdiri dari dua area, yaitu area pusat data dan area pengguna. Pada area pusat data, terdapat tiga kelompok *server* yang dibedakan berdasarkan layanannya, yaitu kelompok layanan *email*, kelompok layanan *domain controller*, dan kelompok layanan lainnya yang berjalan menggunakan sistem virtualisasi. Sementara itu, pada area pengguna terdiri dari komputer-komputer yang dipakai oleh pegawai pada organisasi tersebut untuk mengakses layanan yang disediakan oleh pusat data.



Gambar 3. Topologi infrastruktur pusat data organisasi XYZ

Setelah mendapatkan topologi infrastruktur, dilakukan identifikasi kerentanan yang terdapat pada aset. Beberapa kerentanan yang berhasil diidentifikasi terdapat pada Tabel 1.

Kerentanan tersebut dikelompokkan berdasarkan layanan dan aset yang terdapat di jaringan pusat data.

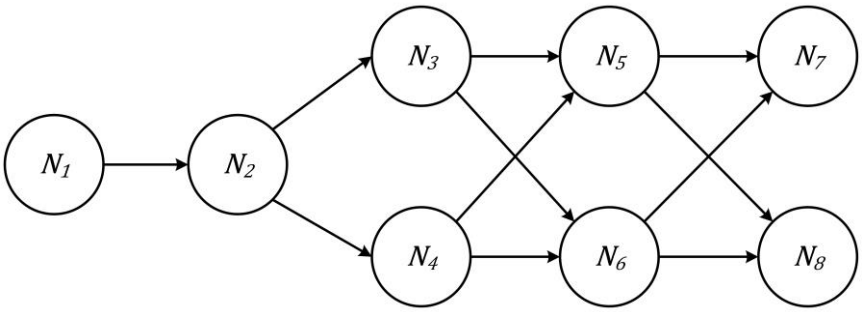
Tabel 1. Daftar kerentanan yang teridentifikasi

Aset	Identitas Kerentanan	Deskripsi
Exchange	CVE-2021-26855	Kerentanan SSRF yang memungkinkan penyerang mengirim permintaan HTTP tanpa melewati proses autentikasi yang sah.
	CVE-2021-26857	Kerentanan yang dapat meningkatkan level akses di lokal perangkat ke hak yang lebih istimewa.
	CVE-2021-26858	Kerentanan yang dapat menyebabkan penyerang untuk membuat *file web shell* yang berisi kode berbahaya dan mengeksekusi *file* tersebut.
	CVE-2021-27065	Kerentanan yang dapat menyebabkan penyerang untuk membuat *file web shell* yang berisi kode berbahaya dan mengeksekusi *file* tersebut.
Domain controller	CVE-2021-36942	Kerentanan yang dapat digunakan untuk mencuri hash NTLM dari *domain controller*.
	CVE-2021-42278	Kerentanan yang terjadi karena kegagalan Active Directory untuk memvalidasi atribut sehingga dapat meningkatkan hak istimewa (*privilege rights*) menjadi Admin Domain.
Workstation (*Client/Server*)	CVE-2017-0144	Kerentanan pada *Server* Message Block 1.0 (SMBv1) yang memungkinkan penyerang melakukan RCE di perangkat target.
	CVE-2021-34527	Kerentanan pada *service* Windows Print Spooler yang memungkinkan penyerang melakukan RCE di perangkat target.

2.3 Pemodelan Serangan dengan Bayesian Network

Pada tahap ini, dilakukan pemodelan serangan dari sudut pandang penyerang yang melakukan serangan dengan cara mengeksploitasi kerentanan di setiap aset. Gambar 4 merupakan jalur serangan yang dimodelkan ke dalam hubungan kausalitas BN. Skenario serangan dibuat berdasarkan teknik dan prosedur yang dipakai pada serangan HAFNIUM. Target serangan utama dari skenario tersebut adalah *server domain controller* yang merupakan suatu aset kritikal bagi sebuah organisasi. Setelah target utama berhasil tereksploitasi, penyerang lebih leluasa untuk menyebarkan *ransomware* ke aset lainnya, baik pada perangkat yang berada di jaringan pusat data maupun di jaringan pengguna.

https://doi.org/10.31849/digitalzone.v14i1. 13788



Gambar 4. Model BN Serangan *Ransomware* dari Kerentanan yang berhasil teridentifikasi

Setiap simpul dalam model BN menggambarkan kerentanan-kerentanan yang harus dieksploitasi oleh penyerang dalam melancarkan serangannya. Pada setiap simpul N_i terdapat probabilitas diskrit simpul (P_{dn}) yang menggambarkan seberapa besar kerentanan tersebut akan dieksploitasi. Nilai P_{dn} pada setiap N_i, didefinisikan sebagai berikut:

$$P_{dn}(N_i) = EPSS_{N_i} \tag{2}$$

di mana $EPSS_{N_i}$ merupakan skor EPSS pada kerentanan pada simpul N_i sesuai dengan kondisi pada 1 Maret 2023. Tabel 2 menjelaskan daftar simpul, identitias kerentanan, dan nilai P_{dn} sesuai dengan fase serangan.

Tabel 2. Daftar kerentanan yang teridentifikasi

Fase Serangan	Simpul	Identitas Kerentanan	P_{dn}
Initial access	N_1	CVE-2021-26855	0.97
Privilege escalation	N_2	CVE-2021-26857	0.31
Execution	N_3	CVE-2021-26858	0.31
	N_4	CVE-2021-27065	0.62
Lateral movement	N_5	CVE-2021-36942	0.26
	N_6	CVE-2021-42278	0.02
Exfiltration	N_7	CVE-2017-0144	0.96
	N_8	CVE-2021-34527	0.25

Dari model BN yang berhasil dibentuk, terdapat beberapa jalur yang dapat dicapai untuk mencapai simpul target. Dalam jalur yang menghubungkan setiap simpul, terdapat ketentuan di mana kerentanan pada simpul tertentu akan dieksploitasi jika kerentanan pada simpul sebelumnya telah dieksploitasi. Ketentuan tersebut mengakibatkan setiap simpul memiliki distribusi probabilitas bersyarat yang bergantung pada simpul yang dieksploitasi sebelumnya. Misalkan N mewakili nilai dari beberapa kerentanan sehingga $N = \{N_1, N_2, \dots, N_n\}$ dan $Parents(N_i)$ merupakan suatu himpunan simpul induk dari N_i, maka probabilitas bersyarat dari N_i dinotasikan sebagai $Pr(N_i|Parents(N_i))$. Lalu, untuk menghitung distribusi probabilitas gabungan (*joint probability distribution*) pada simpul N_i dihitung melalui perkalian *product* probabilitas bersyarat dari N_i dengan formulasi sebagai berikut:

$$Pr(N_1, N_2, \dots, N_n) = \prod_{i=1}^{n} Pr\left(N_i \middle| Parents(N_i)\right) \tag{3}$$

Dalam skenario serangan yang telah dimodelkan, setiap kemungkinan jalur serangan hanya mengeksploitasi satu kerentanan di masing-masing fasenya. Dengan demikian, jika terdapat lebih dari satu sisi yang mengarah ke suatu simpul, maka pada simpul tersebut berlaku peristiwa dijungsi. Kemudian, peristiwa disjungsi tersebut dianalogikan seperti kondisi *OR-gate* pada analisis *fault tree* [21], sehingga perhitungan CPT pada simpul dengan lebih dari satu sisi dirumuskan sesuai dengan Tabel 3. Di mana N_i pada CPT merupakan simpul anak, sedangkan N_{i-1} dan N_{i-2} merupakan simpul induk yang mempunyai sisi yang mengarah langsung ke N_i.

Tabel 3. Perumusan CPT pada simpul N_i yang mempunyai lebih dari satu sisi

Induk		N_i	
N_{i-1}	N_{i-2}	$Pr(c=0\|F)$	$Pr(c=1\|T)$
0	0	1	0
1	0	$1-N_i$	N_i
0	1	$1-N_i$	N_i
1	1	$1-N_i$	N_i

3. Hasil dan Pembahasan

Pada bagian ini, dibahas hasil perhitungan probabilitas serangan dari struktur BN yang telah dimodelkan. Probabilitas serangan menggambarkan nilai paparan risiko dari setiap serangan yang mengancam aset. Perhitungan probabilitas serangan menggunakan formulasi distribusi probabilitas gabungan sesuai dengan yang dirumuskan pada Persamaan 3. Setelah hasil perhitungan didapatkan, skenario serangan dibahas dengan mendetailkannya ke dalam fase-fase serangan. Selain didetailkan pada setiap fase serangan, dibahas juga probabilitas gabungan setiap skenario jalur serangan yang melewati semua fase serangan. Jalur serangan yang memiliki probabilitas yang tinggi lebih mungkin terpapar serangan *ransomware* dibandingkan jalur serangan yang memiliki probabilitas yang rendah.

3.1. Eksploitasi Kerentanan pada Setiap Fase

3.1.1. Fase *Initial Access*

Pada fase *initial access*, penyerang melakukan eksploitasi terhadap kerentanan CVE-2021-26855 yang dinotasikan pada simpul N_0. Berdasarkan CPT pada Tabel 4, probabilitas penyerang untuk mengeksploitasi kerentanan pada fase ini sangat tinggi sebesar 0.97. Hal tersebut mengingat kerentanan pada fase awal ini merupakan kerentanan berjenis SSRF yang dapat diakses dari internet oleh siapa saja. Kerentanan ini diketahui terdapat pada Microsoft Exchange yang populer dikenal sebagai ProxyLogon. Penyerang dapat melakukan eksploitasi pada sistem Microsoft Exchange tanpa harus melalui sistem autentikasi dengan melakukan SSRF sebelum proses autentikasi diterapkan.

Tabel 4. CPT untuk simpul N_1

c	$Pr_{N_1}(c=0\|F)$	$Pr_{N_1}(c=1\|T)$
1	0.03	0.97
0	1	0

3.1.2. Fase *Privilege Escalation*

Pada fase *privilege escalation*, penyerang telah berhasil masuk ke sistem dan berusaha untuk meningkatkan hak akses yang dimilikinya ke level yang lebih tinggi. Kerentanan yang dieksploitasi pada tahap ini adalah CVE-2021-26857 dengan notasi simpul N_2. Tabel 5 menjelaskan probabilitas simpul tersebut dengan nilai sebesar 0.31. Apabila dirangkai dengan peristiwa eksploitasi pada fase sebelumnya, maka probabilitas bersama skenario serangan tersebut adalah 0.30. Dengan menjalani skenario tersebut, penyerang akan mendapatkan hak istimewa untuk melakukan RCE sebagai akun pengguna SYSTEM.

Tabel 5. CPT untuk simpul N_2

N_1	$Pr_{N_2}(c=0\|F)$	$Pr_{N_2}(c=1\|T)$
1	0.69	0.31
0	1	0

3.1.3. Fase *Execution*

Fase *execution* mempunyai ciri khas untuk menghasilkan kode yang dapat dijalankan pada sistem lokal melalui RCE. Pada fase ini terdapat dua simpul kerentanan yang dapat dieksploitasi oleh penyerang. Tabel 6 menjelaskan probabilitas dua simpul kerentanan tersebut, di mana probabilitas simpul N_4 lebih besar dibandingkan dengan simpul N_3. Simpul N_4

https://doi.org/10.31849/digitalzone.v14i1. 13788

merupakan serangan untuk mengeksploitasi kerentanan CVE-2021-27065 yang mengizinkan penyerang untuk mengunggah *web shell* berbahaya dan dapat dieksekusi dari jarak jauh. Jika kerentanan pada simpul N_4 dieksploitasi dengan melakukan serangan kerentanan pada simpul N_2, maka didapatkan probabilitas gabungan sebesar 0.19. Apabila kerentanan pada simpul N_4 dibandingkan dengan kerentanan pada simpul N_3, probabilitas gabungan N_3 terbilang lebih kecil yaitu sebesar 0,096. Dengan demikian, kerentanan CVE-2021-27065 lebih rentan untuk dieksploitasi pada fase *execution*, sehingga organisasi harus memprioritaskan langkah mitigasi kerentanan ini dibandingkan dengan kerentanan CVE-2021-26858.

Tabel 6. CPT untuk simpul N_3 dan N_4

N_2	N_3		N_4	
	$Pr_{N_3}(c=0\|F)$	$Pr_{N_3}(c=1\|T)$	$Pr_{N_4}(c=0\|F)$	$Pr_{N_4}(c=1\|T)$
1	0.69	0.31	0.38	0.62
0	1	0	1	0

3.1.4. Fase *Lateral Movement*

Fase *lateral movement* digunakan penyerang untuk menemukan aset yang lebih kritikal pada suatu organisasi. Penyerang melakukan pemindaian dari sistem yang telah terinfeksi pada fase serangan sebelumnya. Dalam struktur model, fase *lateral movement* dilakukan dari lingkungan sistem Microsoft Exchange untuk menemukan *server domain controller*. Berdasarkan Tabel 7 terdapat dua simpul kerentanan yang berhasil teridentifikasi pada *server domain controller*, yaitu CVE-2021-36942 pada simpul N_5 dan CVE-2021-42278 pada simpul N_6.

Tabel 7. CPT untuk simpul N_5 dan N_6

N_3	N_4	N_5		N_6	
		$Pr_{N_5}(c=0\|F)$	$Pr_{N_5}(c=1\|T)$	$Pr_{N_6}(c=0\|F)$	$Pr_{N_6}(c=1\|T)$
0	0	1	0	1	0
1	0	0.74	0.26	0.98	0.02
0	1	0.74	0.26	0.98	0.02
1	1	0.74	0.26	0.98	0.02

Apabila probabilitas diskrit kedua simpul tersebut dibandingkan, kemungkinan penyerang untuk mengeksploitasi kerentanan pada simpul N_5 lebih mudah dilakukan dibandingkan dengan kerentanan pada simpul N_6. Dengan kata lain, teknik eksploitasi *domain controller* dengan mengambil informasi hash NTLM memiliki peluang eksploitasi lebih tinggi dibandingkan dengan memanfaatkan kerentanan yang terjadi karena kegagalan *domain controller* untuk memvalidasi atribut-atribut tertentu.

Kemudian, jika kerentanan pada simpul N_5 dieksploitasi dengan melakukan serangan pada kerentanan simpul N_3, maka probabilitas gabungan skenario serangan tersebut sebesar 0.081. Dengan membandingkannya dengan skenario serangan dengan mengeksploitasi simpul N_4 terlebih dahulu sebelum mengeksploitasi simpul N_5, dapat disimpulkan bahwa skenario eksploitasi simpul induk N_4 memiliki tingkat kemungkinan yang lebih tinggi, yaitu sebesar 0.161. Oleh karena itu, organisasi harus memprioritaskan langkah mitigasi pada kerentanan CVE-2021-36942. Terlebih lagi, organisasi harus mewaspadai skenario serangan dengan mengeksploitasi kerentanan CVE-2021-27065 yang dilakukan pada fase sebelumnya yang memiliki probabilitas gabungan lebih besar dibandingkan dengan skenario eksploitasi kerentanan CVE-2021-26858.

3.1.5. Fase *Exfiltration*

Pada fase *exfiltration*, penyerang melakukan aksi tipikal serangan *ransomware*, yaitu melakukan enkripsi data pada aset organisasi. Pada beberapa kasus tertentu, penyerang juga melakukan pencurian data tersebut dan menjualnya di beberapa forum. Hal tersebut diakibatkan dari efek serangan pada fase *lateral movement* yang membuat penyerang lebih leluasa untuk mengeksploitasi sistem dengan menggunakan hak akses administrator *domain controller*. Berdasarkan struktur model, pada fase ini penyerang melakukan eskploitasi kerentanan yang

terdapat pada dua area, yaitu area pusat data dan area pengguna. Aset pada area pusat data terdiri dari *server-server* virtual yang tergabung pada *cluster* Hyper-V, sedangkan aset pada area pengguna merupakan komputer personal yang dipakai pegawai untuk melakukan pekerjaan mereka. Aset-aset pada kedua area tersebut merupakan aset yang tergabung pada domain yang dikelola oleh *server domain controller*.

Tabel 8. CPT untuk simpul N_7 dan N_8

N_5	N_6	N_7		N_8	
		$Pr_{N_7}(c=0\|F)$	$Pr_{N_7}(c=1\|T)$	$Pr_{N_8}(c=0\|F)$	$Pr_{N_8}(c=1\|T)$
0	0	1	0	1	0
1	0	0.04	0.96	0.75	0.25
0	1	0.04	0.96	0.75	0.25
1	1	0.04	0.96	0.75	0.25

Tabel 8 menjelaskan probabilitas simpul kerentanan yang dapat dieksploitasi pada fase *exfiltration*. Probabilitas penyerang pada simpul N_7 lebih besar dibandingkan dengan simpul N_8. Probabilitas eksploitasi di simpul N_7 sangat tinggi, yaitu sebesar 0.96. Sementara itu, probabilitas eksploitasi di simpul N_8 berbeda jauh dengan N_7, hanya sebesar 0.25. Artinya, penyerang akan lebih mungkin untuk mengeksploitasi kerentanan aset di area pengguna menggunakan kerentanan CVE-2017-0144. Organisasi dapat mengambil langkah mitigasi dengan melakukan prioritas pada area pengguna terlebih dahulu. Selain itu, organisasi perlu mencermati kerentanan yang dieksploitasi pada fase *lateral movement*. Skenario serangan dengan mengeksploitasi kerentanan CVE-2021-36942 terlebih dahulu sebelum fase *exfiltration* memiliki probabilitas gabungan terbesar yaitu 0.249. Probabilitas tersebut memiliki tingkat kemungkinan serangan lebih besar dibandingkan dengan skenario eksploitasi kerentanan CVE-2021-42278 yang probabilitas gabungannya hanya sebesar 0.019.

3.2. Probabilitas Gabungan pada Setiap Jalur Serangan

Tabel 9. Jalur serangan dan nilai probabilitas gabungannya

Skenario	Jalur Serangan	Nilai Probabilitas
AP_1	$N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_5 \rightarrow N_7$	0.023267
AP_2	$N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_5 \rightarrow N_8$	0.006059
AP_3	$N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_6 \rightarrow N_7$	0.001790
AP_4	$N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_6 \rightarrow N_8$	0.000466
AP_5	$N_1 \rightarrow N_2 \rightarrow N_4 \rightarrow N_5 \rightarrow N_7$	0.046534
AP_6	$N_1 \rightarrow N_2 \rightarrow N_4 \rightarrow N_5 \rightarrow N_8$	0.012118
AP_7	$N_1 \rightarrow N_2 \rightarrow N_4 \rightarrow N_6 \rightarrow N_7$	0.003580
AP_8	$N_1 \rightarrow N_2 \rightarrow N_4 \rightarrow N_6 \rightarrow N_8$	0.000932

Berdasarkan model BN, terdapat banyak pilihan jalur serangan yang setidaknya mengeksploitasi satu simpul kerentanan pada setiap fasenya. Pada bagian ini, dihasilkan daftar semua pilihan jalur serangan untuk membandingkan probabilitas gabungan antar jalur serangan. Tabel 9 menjelaskan semua jalur serangan yang mungkin dapat ditempuh oleh penyerang untuk mengeksploitasi aset di semua fase serangan beserta nilai probabilitas gabungannya

Terdapat delapan opsi skenario yang dapat dilakukan oleh penyerang dalam melakukan serangan *ransomware* pada aset organisasi. Pada dua fase awal serangan, penyerang hanya memiliki satu pilihan kerentanan untuk dieksploitasi sehingga probabilitas gabungannya bernilai sama. Dari semua opsi serangan, skenario serangan AP_5 memiliki probabilitas gabungan yang terbesar. Skenario serangan tersebut secara berantai mengeksploitasi kerentanan CVE-2021-26855, CVE-2021-26857, CVE-2021-27065, CVE-2021-36942, dan CVE-2017-0144. Jika mengamati probabilitas diskrit di masing-masing fase serangan, kerentanan yang dieksploitasi pada skenario AP_5 merupakan kerentanan-kerentanan yang memiliki probabilitas terbesar pada

https://doi.org/10.31849/digitalzone.v14i1. 13788

fase masing-masing. Oleh karena itu, organisasi dapat memprioritaskan langkah mitigasi hanya dengan melihat probabilitas diskrit di setiap fase serangan.

3.3. Evaluasi Hasil Penilaian Risiko

Dari proses penilaian risiko yang telah dilakukan, model yang dihasilkan dapat memberikan gambaran untuk organisasi dalam memprioritaskan penanganan terhadap kerentanan aset yang sewaktu-waktu dapat dieksploitasi oleh serangan *ransomware*. Prioritas penanganan risiko bisa didekomposisi berdasarkan fase serangan. Tabel 10 merupakan daftar prioritas penanganan dari celah kerentanan yang berhasil teridentifikasi pada penelitian ini. Pada tabel tersebut, disajikan daftar prioritas penanganan berdasarkan probabilitas diskrit masing-masing celah kerentanan. Jika terdapat besaran probabilitas yang sama, maka prioritas penanganan dilakukan dengan melihat dari sudut pandang fase serangan.

Tabel 10. Daftar prioritas penanganan berdasarkan celah kerentanan

Prioritas	Identitas Kerentanan	Nama Aset
1	CVE-2021-26855	Exchange
2	CVE-2017-0144	*Client Workstation*
3	CVE-2021-27065	Exchange
4	CVE-2021-26857	Exchange
5	CVE-2021-26858	Exchange
6	CVE-2021-36942	*Domain controller*
7	CVE-2021-34527	*Server Workstation*
8	CVE-2021-42278	*Domain controller*

Selanjutnya, organisasi dapat memberikan tindak lanjut penilaian risiko melalui langkah-langkah mitigasi sebagai bentuk pencegahan serangan *ransomware*. Dalam proses manajemen risiko keamanan informasi, langkah preventif merupakan tindakan untuk mencegah terjadinya serangan siber yang dapat menimbulkan kerugian untuk organisasi. Bentuk langkah preventif yang dapat dilakukan oleh organisasi dapat berupa menutup celah kerentanan yang berhasil teridentifikasi. Organisasi dapat melakukan instalasi pembaruan perangkat yang mengandung *patch* keamanan yang dikeluarkan secara berkala oleh produsen perangkat.

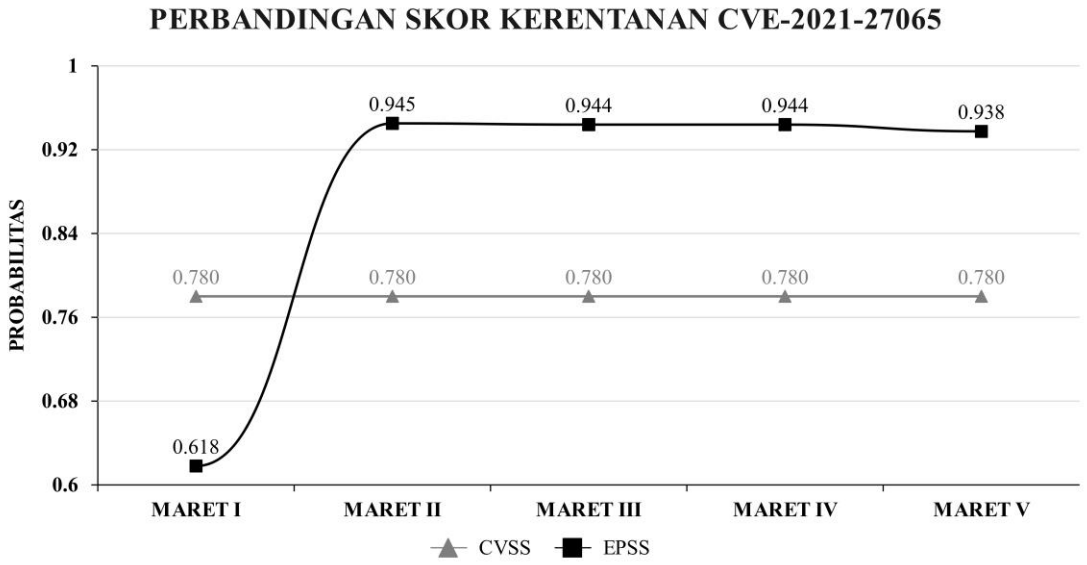
Selain dengan melakukan pembaruan perangkat, organisasi dapat melakukan tindakan-tindakan yang dapat menutup akses masuk ke celah kerentanan perangkat. Misalnya, pembatasan akses ke perangkat atau aplikasi yang memerlukan hak akses khusus dengan menggunakan Multi-Factor Authentication (MFA). Organisasi juga dapat memberlakukan pembatasan koneksi jaringan ke aset-aset tertentu dengan melakukan konfigurasi *firewall* dan penutupan port atau protokol yang tidak digunakan.

3.4. Perbandingan Metode Penilaian Risiko dengan Penelitian Terdahulu

Pada bagian ini dibahas perbedaan metode dan hasil dari penelitian ini dengan membandingkannya dengan penelitian penilian risiko pada layanan *cloud* [16] yang sama-sama menggunakan metode pemodelan BN. Pada penelitian layanan *cloud* tersebut, risiko dinilai melalui skor kerentanan CVSS dengan mengkonversikan nilainya ke skor probabilitas paparan risiko. Skor CVSS yang berada pada rentang 0-10 dikonversi ke skor probabilitas dengan rentang 0-1. Sementara itu, pada penelitian ini paparan risiko dinilai dengan menggunakan skor kerentanan EPSS yang tidak lagi memerlukan proses konversi skor kerentanan. Jika penggunaan kedua skor tersebut dibandingkan, maka penghitungan nilai paparan risiko pada sebuah kerentanan dengan menggunakan EPSS lebih mudah dan efisien. Organisasi hanya perlu mengumpulkan skor EPSS dari API yang telah disediakan tanpa memerlukan proses konversi skor kerentanan.

Selain dari aspek kemudahan penggunaan, penggunaan EPSS pada penelitian ini juga lebih mencerminkan keadaan tingkat probabilitas suatu celah kerentanan perangkat pada waktu-waktu tertentu. Apabila dibandingkan dengan tingkat probabilitas paparan risiko CVSS yang nilainya selalu tetap dari waktu ke waktu, skor kerentanan EPSS mencerminkan tingkat probabilitas yang dapat berubah-ubah mengikuti data faktual yang dikumpulkan dari berbagai macam sumber. Sebagai contoh, dilakukan komparasi skor probabilitas paparan risiko

kerentanan CVE-2021-27065 yang merupakan salah satu kerentanan teridentifikasi pada penelitian ini. Kerentanan tersebut dibandingkan skor probabilitasnya antara penelitian yang menggunakan CVSS dan penelitian ini yang menggunakan EPSS.



Gambar 5. Perbandingan nilai probabilitas paparan risiko pada kerentanan CVE-2021-26855 dengan menggunakan CVSS dan EPSS

Gambar 5 menunjukkan perbandingan nilai dua skor kerentanan tersebut selama bulan Maret 2023. Hasilnya, skor EPSS selalu bernilai fluktuatif berdasarkan waktu pengumpulannya, sedangkan skor CVSS nilainya selalu konstan dari waktu ke waktu. Oleh karena itu, penelitian ini lebih dapat menghasilkan nilai probabilitas paparan risiko yang lebih akurat berdasarkan waktu di mana risiko serangan siber akan dinilai. Dengan demikian, organisasi dapat lebih efektif dan efisien dalam menentukan tindakan mitigasi risiko dari serangan *ransomware* melalui memperkecil tingkat probabilitas serangan pada celah-celah kerentanan perangkat yang mereka miliki.

4. Kesimpulan

Dari pengembangan model ancaman serangan *ransomware* menggunakan Bayesian Network, didapatkan hasil bahwa serangan berantai dengan eksploitasi rantai kerentanan CVE-2021-26855, CVE-2021-26857, CVE-2021-27065, CVE-2021-36942, dan CVE-2017-0144 menjadi jalur serangan yang tingkat probabilitasnya paling tinggi, yaitu sebesar 0.046534. Penelitian ini juga membuktikan bahwa semakin tinggi nilai probabilitas diskrit dari suatu celah kerentanan maka akan membuat semakin tinggi pula tingkat probabilitas dari suatu serangan berantai. Selain itu, penggunaan skor EPSS pada penelitian ini juga membuat penilaian risiko lebih faktual, akurat, dan efektif dibandingkan penilaian risiko dengan menggunakan skor CVSS. Dengan metode pemodelan ancaman yang dikembangkan, serangan *ransomware* yang dilakukan melalui rantai kerentanan dapat lebih mudah diidentifikasi sehingga penilaian risiko menjadi lebih tepat. Dengan demikian, organisasi dapat mengambil langkah yang benar dalam mencegah atau memitigasi risiko serangan siber seperti ancaman *ransomware*.

Apabila dipandang dari sudut manajemen risiko, penelitian ini hanya menggunakan aspek "*likelihood*" sebagai dasar penilaian risiko. Sementara itu, perumusan risiko pada dasarnya merupakan kombinasi dari aspek "*likelihood*" dan "*impact*". "*Impact*" merupakan penilaian seberapa besar dampak serangan dalam memapar suatu aset. Penelitian ke depannya dapat memasukkan faktor "*impact*" tersebut sebagai faktor tambahan dalam penilaian risiko. Dengan demikian, penilaian risiko akan semakin akurat dan bermanfaat bagi organisasi.

https://doi.org/10.31849/digitalzone.v14i1. 13788

Ucapan Terima Kasih
Penelitian ini disponsori oleh Kementerian Komunikasi dan Informatika Republik Indonesia melalui program Beasiswa S2 Dalam dan Luar Negeri Tahun 2021, untuk itu peneliti mengucapkan terima kasih kepada Kementerian Komunikasi dan Informatika Republik Indonesia yang telah memberikan segala macam dukungannya untuk penelitian ini.

Daftar Pustaka

[1] BSSN, "Lanskap Keamanan Siber Indonesia 2022," 2022. [Online]. Available: https://cloud.bssn.go.id/s/3S5B2ToddAFsiXs
[2] I. Nadir and T. Bakhshi, "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques," in *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2018, pp. 1–7. doi: 10.1109/ICOMET.2018.8346329.
[3] A. B. Turner, S. McCombie, and A. J. Uhlmann, "A target-centric intelligence approach to WannaCry 2.0," *Journal of Money Laundering Control*, vol. 22, no. 4, pp. 646–665, 2019, doi: 10.1108/JMLC-01-2019-0005.
[4] U. Tatar, B. Nussbaum, Y. Gokce, and O. F. Keskin, "Digital force majeure: The Mondelez case, insurance, and the (un)certainty of attribution in cyberattacks," *Bus Horiz*, vol. 64, no. 6, pp. 775–785, 2021, doi: https://doi.org/10.1016/j.bushor.2021.07.013.
[5] FBI, "Conti Ransomware Attacks Impact Healthcare and First Responder Networks," 2021. [Online]. Available: https://www.ic3.gov/Media/News/2021/210521.pdf
[6] N. Kshetri and J. Voas, "Ransomware: Pay to Play?," *Computer (Long Beach Calif)*, vol. 55, no. 3, pp. 11–13, 2022, doi: 10.1109/MC.2021.3126529.
[7] NCSC, "Alert: Targeted ransomware attacks on the UK education sector by cyber criminals," 2020. [Online]. Available: https://www.ncsc.gov.uk/files/20200917-Alert-Academia-Ransomware.pdf
[8] Z. Wang *et al.*, "Automatically Traceback RDP-Based Targeted Ransomware Attacks," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018, doi: 10.1155/2018/7943586.
[9] T. Lam and H. Kettani, "PhAttApp: A Phishing Attack Detection Application," in *Proceedings of the 2019 3rd International Conference on Information System and Data Mining*, in ICISDM 2019. New York, NY, USA: Association for Computing Machinery, 2019, pp. 154–158. doi: 10.1145/3325917.3325927.
[10] P. O'kane, S. Sezer, and D. Carlin, "Evolution of ransomware," 2018, doi: 10.1049/iet-net.2017.0207.
[11] ENISA, "MICROSOFT EXCHANGE VULNERABILITIES: Situation update and mitigation," 2021. [Online]. Available: https://www.enisa.europa.eu/publications/situational-report-on-microsoft-exchange-vulnerabilities
[12] S. G. Abbas *et al.*, "Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach," *Sensors*, vol. 21, no. 14, 2021, doi: 10.3390/s21144816.
[13] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces," *Int J Inf Secur*, vol. 21, no. 3, pp. 509–525, 2022, doi: 10.1007/s10207-021-00566-3.
[14] A. Zulfia, E. L. Ruskan, and P. Putra, "Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya," *JOINS (Journal of Information System)*, vol. 6, no. 1, pp. 40–47, 2021, doi: 10.33633/joins.v6i1.4088.
[15] A. Khamparia and B. Pandey, "Threat driven modeling framework using petri nets for e-learning system," *Springerplus*, vol. 5, no. 1, p. 446, 2016, doi: 10.1186/s40064-016-2101-0.

[16] A. Zimba, H. Chen, and Z. Wang, "Bayesian network based weighted APT attack paths modeling in cloud computing," *Future Generation Computer Systems*, vol. 96, pp. 525–537, 2019, doi: 10.1016/j.future.2019.02.045.
[17] J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, and M. Roytman, "Exploit Prediction Scoring System (EPSS)," *Digital Threats*, vol. 2, no. 3, 2021, doi: 10.1145/3436242.
[18] Z. Tian *et al.*, "Real-Time Lateral Movement Detection Based on Evidence Reasoning Network for Edge Computing Environment," *IEEE Trans Industr Inform*, vol. 15, no. 7, pp. 4285–4294, 2019, doi: 10.1109/TII.2019.2907754.
[19] G. McDonald, P. Papadopoulos, N. Pitropakis, J. Ahmad, and W. J. Buchanan, "Ransomware: Analysing the Impact on Windows Active Directory Domain Services," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030953.
[20] N. Ullah *et al.*, "Metrics for Assessing Overall Performance of Inland Waterway Ports: A Bayesian Network Based Approach," 2019, doi: 10.1155/2019/3518705.
[21] R. Duan and J. Fan, "Reliability Evaluation of Data Communication System Based on Dynamic Fault Tree under Epistemic Uncertainty," *Math Probl Eng*, vol. 2014, p. 674804, 2014, doi: 10.1155/2014/674804.