**PENDAHULUAN**

*Malware*, atau *Malicious Software*, merupakan suatu definisi yang diberikan

untuk setiap program atau file atau kode yang dapat membahayakan suatu sistem.

*Malware* berusaha menyerang, merusak, atau menonaktifkan komputer, sistem

komputer, jaringan, tablet, dan perangkat seluler, sering kali dengan mengambil

sebagian kendali atas operasi perangkat. *Malware* menjadi salah satu ancaman yang

paling besar dalam insiden keamanan informasi. Berdasarkan riset dari *Verizon Data*

*Breach Investiogation Report* 2017, aktivitas insiden yang melibatkan *malware*

menduduki peringkat kedua. Pada riset tersebut juga menyebutkan bahwa aktivitas

insiden *malware* menyebabkan kehilangan data dan kerugian finansial yang cukup

signifikan. *Malware* modern saat ini kebanyakan bukan bertujuan untuk merusak,

namun lebih ke arah pencurian data sensitif. Adapun *malware* yang menyebabkan

kerusakan dan kehilangan data biasanya berupa *ransomware*, yang mengancam *user*

yang menjadi korban untuk membayar sejumlah tebusan jika tidak ingin datanya hilang.

**2. TUJUAN**

Secara umum, tujuan panduan ini dimaksudkan untuk membantu organisasi

memahami tentang penanganan suatu insiden yang disebabkan oleh *malware*.

Penanganan insiden *malware* yang dilakukan dengan tepat dan cepat, akan sangat

bermanfaat untuk mengurangi resiko yang diakibatkan oleh *malware* tersebut.

Sedangkan secara khusus adalah sebagai berikut:

a. Memastikan adanya sumber daya yang memadai untuk menangani insiden yang

terjadi;

b. Melakukan pengumpulan informasi yang akurat;

c. Meminimalisir dampak dari insiden;

d. Mencegah adanya insiden lanjutan dan mencegah kerusakan agar tidak lebih melua