Dark City Overview

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Dark City Overview

While it has been advised not to negotiate with attackers, in such cases as with the City of Baltimore, the cost of mitigation was well over the $80,000, demanded in bitcoin via ransomware.

Paying the attacker the bitcoin can be executed in the form of an act of offensive tactic by attaching malware in the coding, which could identify the attackers and their location but most significantly, redact the payment of the ransom in full.

In the event of a city transportation department's information management system being compromised, in particular, the subway system, by ransomware, therefore, prohibiting fares from being collected, it is in the best interests of the city to respond internally, initially.

A loss estimation analysis can be drafted to project the supporting evidence regarding financial security in doing so. The city should also consider moral and public confidence when weighing this decision such as:

- The loss in confidence and trust of public officials
- The cost of hiring public relations firms
- The cost associated with media engagements in an attempt to control the narrative and rectification.
- The inevitable cutbacks which will occur to overcompensate for loss acquired during the attack, which could induce a public outcry in a already depleting city.

It is in the best interests of the city to make for an monetary allowance for surrounding cities to act on behalf of “dark cities” which have been compromised by attacks.

The system information and records to need to have several sources of backup and remote networking for employees in surrounding cities to access in the case of an attack.

In the case of **transportation**, allocating a backup hard drive and networking system which can operate on a separate power source (surrounding cities, charged generators, satellite, or solar power, networking hardware and hard-drive) systems are essential.

In efforts of an overall policy reformation, Bitcoin must be regulated.

Wi-Fi and Telecommunication

Implementing the use of backup communication methods as seen in the Solar Satellite Telecommunications Network and the Solar Transportation Network with the use of charged generators, satellite, or solar power as secondary methods. The act of rerouting telecommunication signals to ping from alternate towers. In the event of the power outrage or terrorist attack, emergency messaging can be dispatched with the use of these secondary resources.

This would provide critical opportunities for a city to communicate within the government and with it's citizens during an unforeseen modification and allow the city or state to operate normally until primary source have been reestablished.

Solar Satellite Telecommunications Network and the Solar Transportation Network with the incorporation of live digital mapping system displaying electrical, satellite, and solar power sources to established, activity, precise location in the event of an outage and potentially where a redirecting of power sourcing can be used.

Security and Access

Security: physical and digital access can be reset through mass encryption using a positive malware methodology. This can be enforced in the event of cyber attacks as an added reactive security response.

It is essential for cities to have a redirecting resource in place for regarding it's transportation, power and telecommunications networks.

It critical to have multi-system plan in motion. For example, surveying for the attackers one a different power source and preventing it from spreading to another while having a solid backup solution for the citizens on another layer.

It is important for law enforcement and citizens to have these solutions in place to maintain the peace as well as eliminate public unrest.

Policy should permit a buddy-system for surrounding cities to operate on behalf of dark cities during the intermitted processes. Residents can access city websites that would be accessible both on and offline for current updates.

The use of emergency notifications and personal text messaging via satellite or solar powered telecommunication systems is seen as an necessity in an overall plan of discourse.

Backups are key, both digitally and within the compounds of a paper trail.

Ongoing mandatory research should be overseen and regulations must be met within the standards and practices for each city.

Establishing which systems and procedures have been effective in the past and providing city staff with adequate training non-negotiable.

Programs running on the algorithm recording behavior such as Citi-SecureWare Software, serves as back up, as well solar powered generators as apart of the city and state urban planning policy.

Anonemis Research
Simenona Martinez
AnonemisResearch.com