www.pipelinepub.com
Volume 18, Issue 1

Protecting Cellular Infrastructure

By: Mark Cummings, Ph.D., Bill Yeack CSE

Ransomware is a severe threat. Waiting till you are under attack to prepare for it is a big mistake. Every organization needs to prepare for ransomware now.

Bace Cybersecurity Institute (BCI) is a nonprofit that has assembled a group of experts to develop an outline that all organizations can follow to prepare for ransomware.

Ransomware attacks can target enterprises, public utilities, government agencies, political parties, schools, hospitals, and more. Attackers are only concerned with how much money they can extort. So, all kinds of organizations need to be prepared. Preparation through ongoing preparation and management can be organized in four phases, as shown in Figure 1 and as outlined below:

- **RM:** Ransomware management
- **R -2:** Pre-attack phase: ransomware detection, intelligence, communications and defense
- **R -0:** Attack phase: management and response
- **R +2:** Loss minimization phase: asset lock up negotiation and restoration

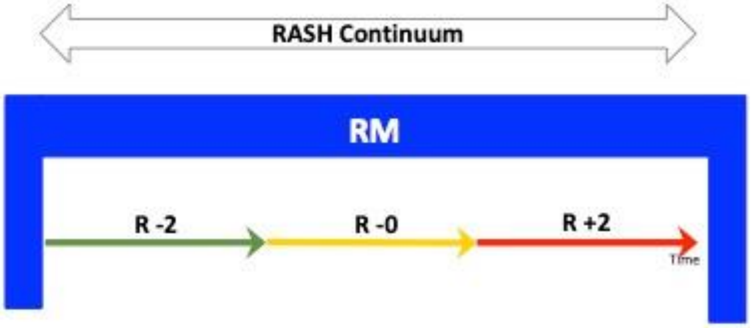

Fig. 1: The RASH Process

We explore each of the ransomware preparation process phases, developed by BCI, in more detail below.

RM - Ransomware Management

Ransomware management is a complex and event-driven process. Unfortunately, you can't protect everything all the time. It is neither economical nor practical. First, the most critical management task is to decide what level of protection should apply for each asset. This ranking needs to be a cooperative effort across the whole organization. Many different parts of the organization will have very different ideas about what needs to be protected. Senior management must weigh in with decisions based upon sound guidelines.

Management must develop plans for "what-if" scenarios. Document the alternatives before you have to decide. Key is planning for the personnel and resource surges for an attack and documenting them, including sourcing.

Ransomware management is a continuous process that needs input from the whole organization while ensuring the confidentiality of the ransomware plans and alternatives. Management must monitor the live-fire training and testing of the entire organization. As a caution, the actual asset list and prioritization must never be used in training.

R -2 (R minus 2): Ransomware Pre-attack Phase

R -2 is the pre-attack phase. The goal of R -2 is to detect, manage, and block potential ransomware threats. The fundamental problem in this phase is the massive amount of data that needs to be analyzed. Yet lurking in the data are indicators of an attack. These indicators or "smells" in the data are very difficult to detect and require sophisticated machine learning tools. When a smell is discovered, it is fed into an attack intelligence system (AIS) that measures the probability of an attack and determines alert levels.

The attack intelligence system has many uses, including providing data to preemptively block impending threats and correct known vulnerabilities; identifying areas to thwart future attacks; detecting successful attacks; and monitoring the tempo of attack for defense resource planning

The AIS also provides the foundation to communicate the organization's alert levels. Communications is the lifeblood of attack management and must include a broad array of participants including senior management, internal technical team members, investors and stakeholders, suppliers, customers, insurance providers, regulators, law enforcement, and media.

Finally, depending on the tempo and velocity of the threat indicators, senior management may take preemptive protective actions. These would include redundancy of locked data or taking specific systems offline and powering them down. These defense response systems are managed by the R -2 team with senior execution approval and include automated tools and manual processes.

R -0 (R minus 0): Ransomware Attack Phase

R -0 is the attack phase. The goal of R -0 is to manage the attack to minimize the total economic impact. The fundamental problem in this phase is time. Everything must be done immediately and in sync as the attack progresses.

As such, the organization needs specific plans with detailed contingencies for responding immediately. These plans should include “what if” action trees, a prioritized list of the top five to ten immediate actions, primary and secondary alternative communication paths for key personnel, and communication plans and resource maps.

The most important issues in the attack phase are the things not to do. These include responding to executives asking for status or communications outside of the attack response plans; attempts to determine the source of the attack; contacting the attackers before a proper negotiation team is in place and prepared to start negotiations, and more. There will be other things not to do that are unique to the organization. Define and prepare for these in advance.

The R -2 team and tool set may have abilities to partially halt and recover from ransomware attacks. Plans for executing recovery should also be in place before an attack.

Planning and preparing for R-0 is a complex and expensive task. Loss containment may be challenging to quantify in advance of an attack, but lack of planning comes at a much higher cost.

R +2 (R plus 2): Ransomware Minimization Phase

R +2 is the post-attack phase. Even with the best advanced detection of smells and R -0 event management and recovery, you may be forced into a position to negotiate with the attackers.

The goal of R +2 is to manage and minimize the total economic impact of the attack. Because of the complexity of these dialogues and negotiations, most organizations should prepare contingency plans and what-if plans for the negotiations. Negotiating with a ransomware attacker is unlike any other negotiation. It is tempting to think that organization’s leadership or staff can successfully negotiate with the attacker. It’s a good idea to remember what a famous lawyer is often quoted as saying, “A lawyer that represents himself has a fool for a client.” Having negotiation support from an experienced ransomware negotiator is critical. As part of the planning process, there should be a clear, mandated way to get this support—either contracted in advance, or via a clear process to quickly obtain this support. This includes a clear mandate that nobody in the organization is to contact the attacker until a proper negotiation team is in place.

Negotiation must include making arrangement for payment. This means acquiring a cryptocurrency, and this may not be as simple as it seems—especially when under attack. In addition to negotiating payment, it's essential to track restoration and assurance that any data exfiltrated will not be passed to others

After the recovery is over, the ransomware process should be updated based on what was learned in the attack.

Continual Ransomware Preparation

Ransomware is a complex and changing threat to organizations today. All organizations need detailed processes and procedures that are constantly maintained. Many organizations may have implemented something similar. But, unfortunately, far too many organizations have poor or incorrect preparation. What is presented here is a very brief overview of a detailed process. If you want to learn more, you may contact BCI for further information and access to its panel of experts.