

Drotos Engineering Disaster Recovery/Business Continunity Playbook



Shane Ẽire Byrne

NTC300

A drawing of a cartoon character

Description automatically generatedHacking (Unauthorized Access)

Hacking: The gaining of unauthorized access to data in a system or computer.

# Disaster Recovery

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Title/Role | Emergency Number | Email | Responsibilities |
| Bob Fletcher | Senior Network Cyber Security Engineer | (858)755-6345 | BFletcher@DrotosEnginnering.com | Mitigation of Initial Attack; Post-Attack Assessment |
| Bill Panthos | Directory of Information Security | (858) 715-1167 | BPanthos@DrotosEnginnering.com | Recovery Efforts |

## Initial Plan of Action

## Upon discovery of infiltration within Dortos’s systems the following actions are to be taken

1. Contact approved personnel in and follow their given instructions.
2. Gather any retrievable information from IDPS.
3. Contain the damage. This involves disconnecting all affected computers from the network, resetting of all passwords, and the immediate execution of approved anti-virus/anti-malware applications; if needed locate and delete all corrupted files and take them off the server(s) to prevent further damage (Jacobson, 2019).
4. Assess the scope of compromise, figure out how many and which systems and/or machines were affected by the attack (Karol, 2013)..
5. Assess what the intruders target was and if was successfully accessed. If a data breach occurred, begin the process of notifying the appropriate parties in the possibility of a breach of their data; if necessary, contact any regulatory agencies (Jacobson, 2019).
6. Remediate and repair systems to prevent further attacks. Reinstall software from their respective master disks (Karol, 2013).

## Troubleshooting and Resolution

* Organize a staff meeting after all other matters regarding the hack have been dealt with; be sure to emphasize security policies based on the nature of the infiltration.
* Investigate any policy compliance violations and deal with as necessary.
* Isolate infected machines and either replace or devise a means of treatment to mitigate the possibility of spreading infections to uninfected systems.
* Engage in penetration testing in order to determine the successfully fix of any vulnerabilities pertaining to the nature of the breach.
* Offer solutions to appropriate personnel in order to deter and mitigate possible future attacks (i.e. honeypots if they are legal in the organization’s residency of operation).
* If not already, encrypt all company data; in possible future attacks this would potentially leave the perpetrator with undeciphered data which would be inherently useless without the appropriate encryption cypher.

## Business Continuity

To restore faith within the organizations clientele after an incident of intrusion within Drotos Engineering’s computer systems and databases.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Title/Role** | **Emergency Number** | **Email** | **Responsibilities** |
| John Wood | Director of Sales | (858) 721-1774 | JWood@Drotosenginnering.com | Recovery Efforts; Contacting affected clients |
| Robert Mumford | Director of Marketing | (858) 742-1992 | RMumford@Drotosengineering.com | Press Releases; Reporting breach to appropriate government entities. |

## Initial Plan of Action

* Contact appropriate personnel appointed to over see the recovery efforts in order to receive instructions for the recovery operation.
* Determine the appropriate parties post-breach and contact affected parties from the breach incident; if possible, inform them of what known information may have been compromised.
* If necessary, contact the appropriate governmental regulatory agencies and provide information pertaining to the breach and what data may have been compromised.
* Respond quickly and honestly about the incident (5W Public Relations, 2020), this may not completely restore the publics faith within the company, but it can lessen the cynicality produced from those affected by the incident.
* Create a public pathway for communication for those affected (5W Public Relations, 2020). Be sure to engage those affected, this will help to get negativity off the company’s main sites. It would behoove the organization to create a new site where detailed information is provided, questions can be answered, and solutions can be addressed (5W Public Relations, 2020).

## Troubleshooting and Resolution

* Communicate with appropriate parties in a clear and concise manner. The company’s credibility could be on the line, it would be in the company’s best interest to address any issues pertaining to the incident.
* Offer information to infected parties. The best means to mediate the situation is to offer services to those affected by the incident. Free credit monitoring, discounts, gift cards, or some other form of compensation (5W Public Relations, 2020).

**References**

5W Public Relations. (2020). 4 WAYS TO ENSURE BEING HACKED DOEN’T TURN INTO A PR

NIGHTMARE. Retrieved from https://www.5wpr.com/new/data-breach-public-relations/

Carew, J. (2018). Business continuity and disaster recovery in the hack economy.

Retrieved from

<http://www.brainstormmag.co.za/technology/14303-business-continuity-and-disaster-recovery-in-the-hack-economy>

Karol, G. (2014). 5 Steps to Recovery After Your Business Has Been Hacked.

 Retrieved from <https://www.foxbusiness.com/features/5-steps-to-recovery-after-your-business-has-been-hacked>

Jacobson, D. (2019). After the Hack: A 10-Step Guide to Restoring Your IT Network Security.

  Retrieved from

<https://www.netstandard.com/after-the-hack-a-10-step-guide-to-restoring-your-it-network-security/>