CYBERSECURITY INCIDENT RESPONSE

In case of a security incident, it is important to know what to do and how to act. ON2IT's Cybersecurity Incident Response Team (CIRT) is prepared to deal with all types of cybersecurity incidents thanks to adequate and efficient procedures, checklists, expertise and training.

CYBERSECURITY INCIDENT RESPONSE PROCESS:

1. **Preparation**
   Communication plans, procedures and handling checklists are periodically tested and updated. Contact with relevant authorities is maintained. Team members are trained to deal with the latest developments on cybersecurity threats.

2. **Identification**
   ON2IT provides advanced automated detection of threats and vulnerabilities in order to proactively alert and take action. Customers can report a security incident 24/7 to our mSOC™. The incident is assessed and triaged by the mSOC™ First Responder. The priority level, severity, and potential impact are determined. CIRT members are informed.

3. **Containment**
   Primary damage control is initiated according to established protocols. Evidence is secured and thorough analysis is performed to identify actual impact and mitigation strategy. Frequent status updates are scheduled with relevant stakeholders to communicate progress and define next steps.

4. **Eradication**
   Clean-up and removal of attack traces, infections or backdoors together with the customer. Additional investigation is performed to determine if other environments are potentially affected as well and require protective measures.

MONITOR
OPERATIONS
REPORTING
CASES
FILER
SERVICE
THREAT EVENTS ANALYSIS
DATA
Average of all Protect Surfaces
(D)DOS
Average of all Protect Surfaces
ENCRYPTION
Average of all Protect Surfaces
ENDPOINT
Average of all Protect Surfaces
IAM /
CLICK HERE TO GIVE FEEDBACK
Search the web and Windows

Escalation

If the mSOC™ analysts determine that the incident has potential major impact on business processes or security, the incident is escalated to ON2IT's CISO who can decide to scale up the CIRT team to a Major Incident Response Team (MIRT).

The MIRT consists of cybersecurity specialists and is established ad hoc in case of a major incident that requires specific and immediate strategic attention, for example in case of involvement of law enforcement or supervisory authorities.

5. **Recovery**
   Bringing systems back to operations together with the customer, and performing a final sanity check to validate mitigation. Systems might be subject to intensified monitoring to detect suspicious behavior.

6. **Post Incident**
   A root cause analysis (RCA) is performed in order to identify improvements and security improvements advisories (SIAs) that aim to avoid the reoccurrence of a similar incident. An evaluation meeting is scheduled to discuss post-mortem analysis, lessons learned and monitor follow-up on SIAs.

Integrity

ON2IT maintains high standards for data and information integrity during the incident. Our teams are trained to work according to established protocols and checklists so that data integrity is maintained during and after an incident. This is essential in order to serve as forensic evidence in case of prosecution.

Expertise

ON2IT has been providing cybersecurity services for over fifteen years. As part of our managed services, we provide 24/7 remote support on incidents with an exclusive focus on incidents related to customer systems and IT operations. Our continuous monitoring solution detects threats that can be analyzed and mitigated proactively by the mSOC™.

Communication

Frequent updates are provided to involved stakeholders. These include:

- Current status of the incident
- Current risk and exposure
- Identification of 'patient zero'
- Timeline of events
- Involvement of third parties
- Mitigation steps that have been taken
- Next steps

INSIGHTS IN CYBERSECURITY INCIDENTS

AUXO™

- Real time incident information
- 24/7 available status updates
- Documented event trails
- Periodic SLA reports

Compliance

Our AUXO portal provides customers with real time visibility and traceability on detailed security event information. This can function as evidence for regulatory bodies, auditors and boards as might be required by the NIS Directive or NIST 800-53 Framework.

HELP! AN INCIDENT!

Don't panic, our mSOC™ is available 24/7 to assist you in case of a security incident.
ON2IT offers worldwide managed cybersecurity services for organizations with complex and dynamic IT infrastructures. Our managed services are modular, scalable, cost-effective, and always based on Zero Trust.

CURIOUS ABOUT YOUR INCIDENT RESPONSE CAPABILITIES? WE WILL HELP YOU FIND OUT.

☎ **CALL (214) 206-8446**

7300 Lone Star Drive / Suite C200 Plano, TX 75024
Email: sales@on2it.net / Phone: (214) 206-8446