

Stability and Security from the Perspective of Global Companies

November 20th, 2013

NIC Costa Rica
Rosalia Morales
Executive Director

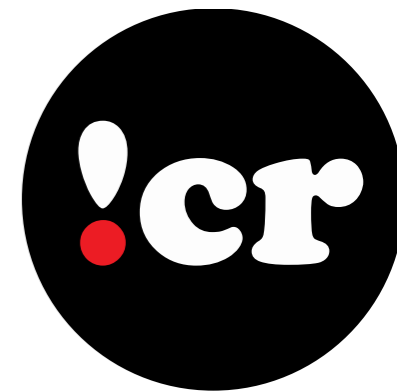


NOVEMBER 20, 2013

AGENDA



- NIC CR Security Incident
- NIC CR Response
- Recommendations



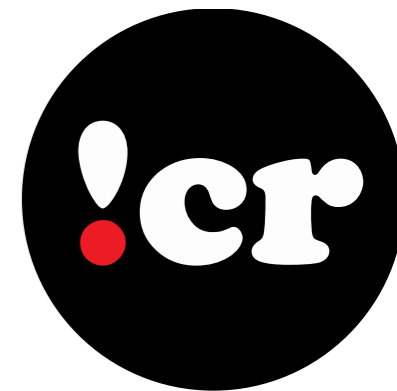
Security Incident

SECURITY INCIDENT: OCTOBER 13, 2013



- **Website vulnerability**
 - Hackers found a vulnerability in the html code of our registry webpage
 - Signed in to Mark Monitor's account
 - Redirected servers of 8 important domains
 - Our system did not report any abnormal behavior
- **Incident**
 - Mark Monitor contacted us about unauthorized changes
 - IT and Client Service responded immediately to request
 - In less than 2 hours all servers were restored
- **DNS Servers were not attacked**





Reaction



SECURITY INCIDENT: REACTION



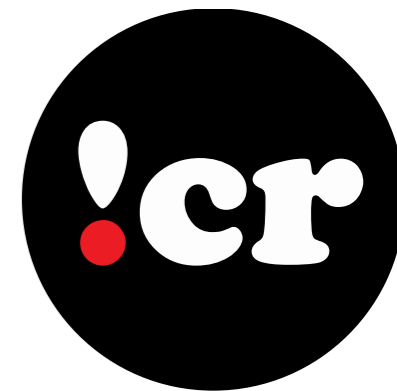
- **Reaction**

- Media interest
- Contacted ICANN Security Team
- Contact CSIRT team of main ISP provider
- Released a public statement clarifying the situation
- Defined 2 spokespeople – clear message to all parties
- Clear message that DNS servers were not compromised
- Operations team supervised and approved all account changes until glitch in webpage was restored

- **Communication with client**

- Clear and transparent
- Updated Mark Monitor on any progress or information they required



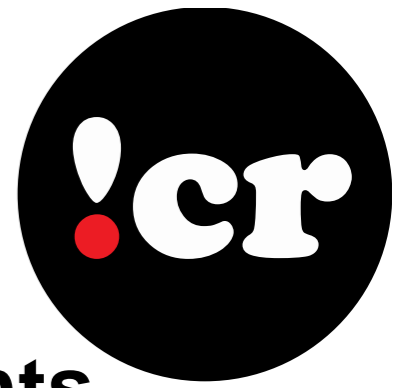


Recommendation

S



RECOMMENDATIONS: FOR OTHER CCTLDS



- **Inmediate and transparent communication with clients**
- **Contact ICANN Security Team for advice and local CERT or CSIRT**
- **Have a clear media strategy**
- **Have an internal security incident protocol**
- **Pre-empt: many security incident experience in the ccTLD community to learn from**



Thanks!