Don’t Just Scratch the Surface When Securing Internal DNS

Data is the Core of Every Business
But as people and things get more connected, targeted attacks can put your data and infrastructure at risk.

Internal DNS Attacks Can Lead to Business Downtime

- **Internal DDoS Attacks**
  - Flood the network with traffic to overwhelm the network or IT teams
  - Can be launched by a malicious insider or an infected endpoint
  - DDoS attacks could cause losses of $100K revenue per hour.¹

- **DNS cache poisoning attack**
  - 66% of China’s DNS infrastructure, with millions of domains inaccessible.²

Advanced Persistent Threats (APTs) and Malware Exploit DNS

- Malicious traffic is visible on 100% of corporate networks.³
- Every 6 minutes a known malware is being downloaded.⁴
- 47% of bots are active for more than 4 weeks.⁴

DNS Can Be Used to Smuggle Your Data

- DNS tunneling attacks let infected endpoints or malicious insiders exfiltrate data.
- Attackers have recently used DNS tunneling in cases involving the theft of millions of accounts.⁵
- 46% of large businesses have experienced DNS exfiltration.⁶

Millions Are at Stake

**That means:**

- **Downtime and lost revenue**
- **Damaged reputation**
- **Lost customers**

**Over 100M records were exposed in first four months of 2015.⁷**

- A recent high-profile data breach is likely to cost more than $100M.⁸

Infoblox helps protect against internal DNS threats.
www.infoblox.com/InternalDNSSecurity

Sources:
2. DNS poisoning slams web traffic from millions in China into the wrong hole, The Register, January 21, 2014
6. DNS attacks putting organisations at risk, survey finds, SC Magazine, December 23, 2014
8. Anthem data breach cost likely to smash $100 million barrier, ZDNet, February 12, 2015