UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERIAS
DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

MATERIA:
SEGURIDAD DE LA INFORMACION

MAESTRO:
FRANCO LOPEZ VELARDE, EMMANUEL

TITULO DE INVESTIGACIÓN:
ACTIVIDAD DE APRENDIZAJE NÚMERO 6: INGLES

FECHA ENTREGA:
LUNES 24 DE SEPTIEMBRE 2018

ALUMNO:
FELIPE DE JESUS RUIZ GARCIA

CODIGO:
214522077

CARRERA: INGENIERIA INFORMATICA (INNI)

SECCION: D02

CALIFICACIÓN Y OBSERVACIONES:

DATABASE SECURITY – RISKS AND CONTROL METHODS

Databases are money, in fact the companies relies all the trademark as o main source of Bussines process. The current bussines model is focus on be online “all through internet” and it cuestion expose the companie’s services a millions of threads. The area between the service that holds the companies databases and the Internet connection is knowed as DMZ or demilitarized zone (sometimes referred to as a perimeter network). Nowadays all service available to the internet are in constantly scanning, looking for vulnerabilities to be exploted. Thinking that our databases are in the In DMZ, a mismatch config or a little wrong configuration could brings terror or break the entere companies. Lets say that we are the administrator for the Important financial startup that provides credits to all the country (like Infonavit or something) and we are focus on make a cool webpage to register user, consults your credits and make some payments. We need take in count a lot of things before that release the page.

First one is “**All must be legal**” and respaldate on contracts and documents signed for the stakeholders: to avoid violate the laws with user collection data, country internet policies and more we need be synced with the all legal actions to avoid legal conflicts.

“Security, then security” :

In the databases servers, install only the software required, NOT MORE, on a operative system stable, configure the service to guarantizate the only local scope,

disable the major accounts possible, set a large and complexity password and chage it every month…. One password for user, service and databases.
Discard all the default settings for everything> e.g. if you need a webservice configure all option to ensure that only authorized user can handle it. Set firewall rules, change default ports. Capture logs. Put a intermediate host or special hardware intended to prevent denegation of service can improve the availibitly.
And Make sure that you are update on all, system, databases and third party libraries.
“If you find a bug before a attackers, then is not a bug anymore”: sandbox technichjial and safe production>
The audits for validate the internal and external process and quality are one of the major important stepts to make sure the bussines is safe.
Make available for internet only software tested, in this way you garantizated the right behavior and your not concernt for weird or unexpected software output.
Ensure the all process, testing and coverity is the shape of the end-users experiment on the fly.
Feedback is to grow: Make channels to support the end-user
Be safe: Masking and encrypt password on databases and all request is a good way to make .
Make backups and register them according dates and content.
Thinking like the attacker, security come more easy.
Backtracking...

SECURITY NEWS

https://www.theguardian.com/us-news/2018/aug/22/dnc-hack-voter-database-detected-fbi

Wed 22 Aug 2018 20.21 BST

DNC detects attempt to hack voter database just months before midterms

The Democratic National Committee has contacted the FBI, but officials say it was not known who was behind the attack

Sabrina Siddiqui in Washington
@SabrinaSiddiqui

Wed 22 Aug 2018 20.21 BST
Last modified on Wed 22 Aug 2018 22.09 BST

This article is over 1 month old
Shares
70
‘This attempt is further proof that there are constant threats as we head into midterm elections and we must remain vigilant in order to prevent future attacks,’ DNC chief security officer Bob Lord said in a statement.
‘This attempt is further proof that there are constant threats as we head into midterm elections and we must remain vigilant,’ the DNC’s chief security officer, Bob Lord, said. Photograph: Mario Tama/Getty Images

The Democratic National Committee (DNC) has contacted the FBI after detecting a possible attempt to hack its voter database, which contains information for tens of millions of voters across America.

The disclosure comes just months before the 2018 midterm elections and marks the latest indication that external powers might still be engaged in active efforts to infiltrate the US electoral process. The news was first reported by CNN and was confirmed by the Guardian.
Kids at hacking conference show how easily US elections could be sabotaged
Read more

It was not immediately known who was behind the latest attempt to penetrate the DNC system, officials said, while noting the effort was thwarted.

“This attempt is further proof that there are constant threats as we head into midterm elections and we must remain vigilant in order to prevent future attacks,” the DNC’s chief security officer, Bob Lord, said in a statement.

“While it’s clear that the actors were going after the party’s most sensitive information – the voter file – the DNC was able to prevent a hack by working with the cyber ecosystem to identify it and take steps to stop it.”

The DNC was at the center of Russian interference in the 2016 presidential election, when hackers illegally

obtained and subsequently leaked thousands of internal emails through WikiLeaks just ahead of the party's national convention. Russian hackers subsequently stole more than 50,000 emails from John Podesta, then the chairman of Hillary Clinton's campaign, and released them in tranches in the months before the November election.

Robert Mueller, the special counsel overseeing the FBI's investigation into Russian meddling in the US election, indicted 12 Russians last month in connection with the DNC and Podesta hacks. The DNC separately filed a lawsuit earlier this year seeking millions in damages from the Russian government, the Trump campaign and WikiLeaks, claiming a widespread conspiracy to influence the 2016 election.

US intelligence officials have repeatedly warned of "pervasive" efforts by Moscow to disrupt the 2018 midterms, even as Donald Trump has shown little regard over the matter. The president ignited a firestorm last month at a summit with the Russian president, Vladimir Putin, in Helsinki, in which Trump sided with the Kremlin over US intelligence authorities on whether Moscow had interfered in the 2016 election. Although Trump later walked back his comments, amid an avalanche of criticism, he has continued to downplay the threat posed by the Russians in a high-profile split from the national security community.

On Tuesday, Microsoft accused the Russian group linked to the hacking of Democrats in 2016 of launching fresh attacks against political groups in the US. The technology company said it had uncovered fake websites designed to mimic two conservative thinktanks and other fake domains purporting to belong to the US Senate.

IN MY OPINION []

The country wars going beyond weapons, this are focus informatics services, and data alteration.
This is a good example of the importance of database... All country elections stored on a databases posibly alterated remotly ? Right now we can not feel security even FBI behind... hackers.
This shows how the vulnerabilites expuses and good practices are mandatory for correct resguard data life.
Keep update.