DominoProtect

This document discusses the benefits of BCC's DominoProtect and how it can save businesses from myriad data related issues. Before we get into the detail, let's look at some high-profile news headlines.

There are on average 400 data-breaches a month reported to the UK Information Commissioner. These are internally reported cases – The Register 14th May 2019

The average fine for a data breach has doubled in one year to £146,000 to September 30th 2018, - RPC Legal 30th October 2018

Three of the largest fines issued by the ICO in the last year were against:

Equifax, which was fined the maximum £500,000 for failing to protect the personal information of up to 15 million UK citizens during a cyber-attack in 2017

Carphone Warehouse, which was fined £400,000 for failing to adequately protect customer and employee data

The British and Foreign Bible Society, which promotes the availability of the Bible worldwide, was fined £100,000 following a cyber-attack that compromised personal data of 417,000 people

Data indicates human error prevailing cause of breaches, incidents - Mahmood Sher-Jan, iapp.org

https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/

With a 20+ year legacy of application development and hosting services under its belt, IBM Notes and Domino can be justly proud of its record and trail-blazing history in workgroup and enterprise wide workflow and collaborative applications that serve every imaginable aspect of business operations.

However, with the number of cyber-attacks increasing year on year, and the risk that human error poses in the majority of unintentional data breaches, organisations would be well advised to consider ways to more actively prevent such issues from occurring, especially since the average fine for such cases is £146,000.

DominoProtect from BCC provides additional security and auditing that far exceeds the native Domino administration tools and log.nsf.

Are you using the Domino ID Vault

The Domino ID vault is a fantastic administrative tool introduced in Domino 8.5 to facilitate the storage and periodic harvesting of Notes User IDs. The ID Vault resides on a Domino server and is secured with the server ID of that server. Consequently, if your server does not have a password on the ID, then the vault cannot be considered secure.

Risks

An attacker could breach the network and obtain copies of the server ID and the ID Vault database.

A rogue administrator would be able to take a copy of the vault and the server ID

In both cases whoever holds both the server ID and the ID vault has all of the cryptographic information necessary to decrypt the IDs within the vault . IBM provides best practice information on securing the vault server but when followed it can make unattended server restarts much trickier than necessary.

Furthermore, the process generally requires that the Administrator is knowledgeable of the password which means it either might be forgotten or perhaps written down, thereby introducing other security risks.

The ‘white knight’ in this scenario is BCC’s DominoProtect software. At its most basic deployment DominoProtect will apply a random password to the Domino server ID. This is stored in an encrypted file on the server’s hard disk, and upon a server restart, the DominoProtect DLL will seamlessly and instantly apply the highly secure password to the challenge/response and allow the Domino server to start up.

The advantages are that

No administrator knows the password, it is not stored in clear text anywhere on the server

If the server’s Notes.INI file is altered to remove DominoProtect, the secure password is still on the Domino server ID

How are Databases Protected?

IBM Domino allows all databases to be secured with the database Access Control List, ACL. However, anyone with manager access has the ability to alter the ACL. Furthermore, an administrator with FullAdminAccess rights to the server can circumvent the database ACL and gain complete access to the database.

Consequently, if you have a database with payroll data, or a HR user management system or even the CEO’s mail file, all can be viewed by a rogue administrator with the correct level of system access, and as seen above, this could constitute a hefty GDPR breach.

With DominoProtect it is a trivial task to lock down access to only the intended users. When an administrator with Full Administration Access attempts to open a secured database, they are prevented from doing so irrespective of their access level in the ACL.

This rogue administrator might be tempted to temporarily turn off such protections within DominoProtect. However, if the system is locked down to a specific DominoProtect Administration ID which itself is protected by multiple passwords, there is no way for the configuration to be changed without at least one other person’s knowledge.

That’s cool, but what about Document and Field level protection?

Obviously, organisations want to give users and administrators the flexibility to do the tasks they are employed to do, but that does not necessarily mean sharing the ‘keys to the kingdom’. For example, with DominoProtect it is possible to prevent users from opening and reading specific documents. When this type of protection is enabled, the applicable users are not even able to view fields via the document properties dialog box.

Taking things a step further, the server document can be protected from updates, or perhaps more usefully, specific fields can be prevented from update. A good use case here might be preventing a change to the Full Access Administration field, again to ensure that administrators are not dipping in to data that they should not have access to.

What happens when higher level access is legitimately required?

Consider the scenario where DominoProtect has been deployed to prevent Administrators having too high an access level to the mail databases of all users, yet for the purposes of restoring messages accidentally deleted by a user, the administrator needs access to the mail file. Well DominoProtect has a Change Control function built right into the system. When setting up the protection rules, a change request subform can be inserted into any form in any database, for example the Group form in the Domino directory.

When the administrator wishes to add his name to the “UserMailfileAdmins” group, they can start the group edit process and then with one click, initiate a change control process. The change request is routed to a nominated approver who will either approve or deny the request. If the request is approved, the change to the group is immediately processed and the administrator is allowed to complete the task at hand.

OK, but what about erroneous changes that need to be reverted?

Continuing with the above example, once the work has been completed, the approver can at a future specified time, e.g. 2 hours after granting the change, open the Change Request log select the change and revert it thereby revoking the Administrator's access and restoring the 'zero access' status of the server.

This logging and restore capability provides a backup in case changes are made that adversely affect any aspect of the environment. For instance, when adjusting parameters to improve performance or implementing a new mail routing topology. Should any change not be beneficial to the environment, not only is there a full change record with accountability, but the respective changes can be swiftly reverted should that be necessary.

Conclusion

BCC's DominoProtect can help any organisation ensure compliance with current legislation. It can remove the risk of a data breach by applying higher security than default. Those who manage teams of administrators will welcome the benefits of accountability and the full audit log of changes

Some organisations would question whether they can afford to add this level of enhancement to their servers, however, in this day and age I would ask, can they afford not to?

Contact

BCC Business Collaboration
Company, Ltd.
Becket House
36 Old Jewry
London, EC2R 8DD
UK Tel: +44 20 32909224

Headquarters
BCC Unternehmensberatung GmbH
Frankfurter Straße 80-82
65760 Eschborn
Germany
Tel: +49 6196 640400

See web link "Securing your Notes ID Vault Server"
https://www-10.lotus.com/ldd/dominowiki.nsf/dx/securing-your-notes-id-vault-server