

浅析数据加密技术在企业工作平台中的应用

曾垂勇 唐娅雯

四川大学锦城学院 四川 成都 611731

【摘要】云计算、大数据等技术的日新月异让计算机的应用更加贴近人们的工作和生活,享受着科技带来的便利的同时信息数据安全的保证也逐渐被人们所关注。数据加密技术也从之前的技术人员关注变为融入了人们平常生活之中,而数据加密技术是保证工作中信息安全的重要手段之一,本文概述了企业工作平台面临的安全威胁,以 link 系统为例浅析了企业工作平台中的数据加密技术以及应用。

【关键词】数据加密技术;企业工作平台;应用

1 引言

随着计算机信息技术以及网络的高速发展,尤其是国际互联网(Internet)的广泛应用,网络中的信息数据安全问题被越来越多的人所提及。再加之计算机已经普遍存在于人们的工作生活中,以及计算机网络本身所具有的互联性、多样性等特质,敦促着人们在使用计算机工作时需要更加地注重信息数据的加密。而工作中的系统文件数据安全、人们的账号私人信息安全,信息数据传输过程中的安全都面临着被恶意的破坏和威胁,信息数据的加密变成了一个必要的过程。

2 数据加密技术的概述

所谓数据加密(Data Encryption)技术是指将一个信息(或称明文, Plain text)经过加密钥匙(Encryption key)及加密函数转换,变成无意义的密文(Cipher text),而接收方则将此密文经过解密函数、解密钥匙(Decryption key)还原成明文。将密文还原为原始明文的过程称为解密,它是加密的反向处理,但解密者必须利用相同类型的加密设备和密钥对密文进行解密。数据加密技术增强了信息数据的隐秘性,从而使得信息数据完整性的安全有了一定的保障。数据加密技术的多样化发展也让现今社会下的很多企业信息数据得到了一定的保障,为企业的发展壮大提供了坚实的后盾。

3 企业工作平台管理现状

随着现代网络安全信息技术的发展,越来越多的企业将信息化管理系统作为公司的工作应用平

台,以进行大规模的信息数据化管理。这样的工作系统既方便管理层进行工作管理操作,也让员工的工作更加的便捷,工作效率得到了很大的提升。此外应用信息化管理系统不仅能够更加清晰高效的完成企业各种信息的分类与整理工作,还能够帮助帮助企业管理人员制定和开展企业活动或企业发展策略,使得企业更好的进行可持续性的发展规划。

但是,企业工作平台的信息化管理系统应用也存在着许多的不足以及面临很多的安全威胁,如企业信息数据的泄露危机、信息数据传输过程中面临的被恶意破坏的威胁、企业工作人员个人信息的安全、操作管理人员的配置不当等。这些信息数据造就了一个企业,也让一个企业有了发展壮大基础,可是一旦这些信息数据泄露或被恶意破坏,那么给企业带来的经济损失是不可估量的,甚至也有可能致命。

另外,各类企业的工作平台实际使用上与企业需求的磨合周期长、可持续性发展能力逐渐变差。平台功能的升级与改进缺少发展动力,企业的需求又在不断的改变,使得工作系统后期维护投入超出系统建设维度,开始出现信息安全漏洞,从而被黑客入侵或其他竞争对手所攻击,导致企业信息数据泄露,造成不可逆转的后果。

4 企业工作平台面临的安全威胁

4.1 工作平台的漏洞

企业的信息化管理工作平台通常具有两种开发模式,一是企业自主开发信息化管理平台,对企业的工作要求有着最高的契合度,另一中是采用第三方

软件厂商的管理系统为企业提供服务。两种开发模式的应用平台都有着广泛的应用,但也有着同样的安全漏洞。如系统底层漏洞不可避免;安全管理软件如防火墙、TCP/IP 协议的漏洞等,如果这些管理平台的配置不当,也会为企业的管理带来安全威胁。

4.2 外部人员的非法入侵或恶意攻击

企业的信息数据在内部大多数以明文形式呈现,方便数据的管理及流通。一般对数据的加密没有那么重视,这样往往面临着被非法窃取的威胁。加之企业信息数据的一大特质——价值高,更加的容易招来外部人员通过非法手段入侵企业工作信息平台,窃取信息,泄露商业机密;或者竞争对手的恶意系统攻击,对信息数据的完整性进行破坏。这些威胁往往都会对企业造成致命性打击。

4.3 管理人员的操作不当

企业的工作平台无论是自主开发还是第三方软件厂商的管理系统为企业提供服务,都需要管理人员去配置和管理系统大局,以达到企业工作上的需求目的。其中管理人员的系统配置不当、管理策略出现错误、对工作平台的使用和维护起了误导作用以及各子系统采用不同的标准和规范导致信息数据的不一致都是引起企业工作平台产生安全漏洞的原因之一。

5 数据加密技术的应用——以 Link 系统为例

信息数据的安全对一个企业工作平台尤为重要,为了保证信息数据的安全,企业必须在工作平台的某些过程或者内部采取数据加密技术,才能保证重要的信息数据不被窃取或者恶意破坏,甚至就算被窃取也不会被非法识别和利用。

5.1 Link 系统的漏洞问题发现

Link 系统在房地产中介大亨链家中占据着举足轻重的地位,这样的一个系统为公司提供了强大的线上网络数据以及多样化的管理工具。管理人员便捷的平面化管理,工作人员的高效数据操作都是在 Link 系统中完成。但这样的一个系统在最初也存在着很多的漏洞。

个人信息的安全在最初并没有得到保证,工作人员的工作账号及密码由系统设定,不能轻易更改,久而久之容易被窃取及利用。而系统内部的一些数

据,如房源详细信息、楼层、物业地址等在最初也是以公共形式出现,这样的信息共享化虽然达到了更好的传播效果,但公司为此建立的房源信息系统也更加的容易被入侵以及竞争对手的恶意破坏及模仿。

5.2 解决办法

5.2.1 统一身份认证系统中加入数据加密技术

统一身份认证系统是集中对用户的信息进行认证管理的一个系统环境,该系统可以管理用户的身份和权限信息,以统一的用户管理、身份认证方式来为不同的应用程序提供服务。统一身份认证系统主要的作用是将用户的登录信息和数据库中的信息进行对比,对客户端的登录请求进行验证,经过验证,若客户端身份信息合法,认证系统则向客户端返回统一的认证标志 (Ticket),同时认证系统需要对认证标志进行验证,保证认证标志的有效性。

统一身份认证系统集中管理了工作人员的信息及权限信息,对个人信息的的安全有了进一步的保证。在统一登陆的节点处,采用单点登陆模型,而单点登陆模型中又可以采用多种数据加密技术以保证工作人员的个人信息安全。统一身份认证及单点登陆模型如图 1 所示:

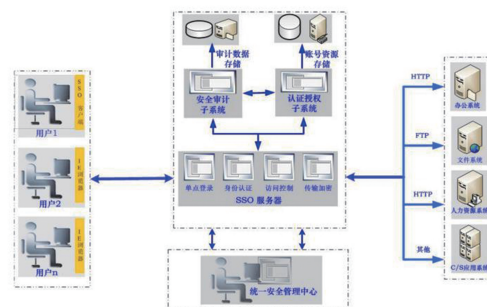


图 1 统一身份认证及单点登陆模型

5.2.2 口令身份认证加密技术

在单点登陆模型的节点处,可以采用口令身份认证数据加密技术,这种数据加密技术普遍存在于各大企业的工作平台中,以满足复杂性原则(复杂性原则为口令必须至少包含大小写字母、数字、特数字符且不少于八位字节长度)的口令帮助用户登陆工作系统,同时不再仅限于系统设定,工作人员可自行设定身份认证口令,这样避免了因口令一致导致员

工个人信息的泄露或者被盗取。Link 系统中的登陆技术也采用了这种口令认证数据加密技术,进一步保证了员工数据安全。

5.2.3 生物识别加密技术

另一种应用在单点登陆节点处数据加密技术为生物识别技术。生物识别技术是利用人体身上不可复制的特质或行为特征,通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合,来进行个人身份的鉴定。这样数据加密技术是将数据存储在一个数据存储池中,用户访问时需要通过已经存入系统数据库中的生物特征如指纹、声纹、虹膜的验证,才能访问系统,才能获得相应的权限。

Link 系统中的统一身份认证数据加密技术还体现在单一数据可被查看性上。Link 系统中的房源业主信息只有单一的专属维护人可以查看,其他工作人员均不能查看,以及房源物业地址等相关详细信息也只有登陆了系统的工作人员才能查看,第三方

访客登陆并不能查看。这是因为统一身份认证系统对登陆人员权限的分配,使得信息数据多了一层加密保护,这也是数据加密技术的一种呈现方式。

统一身份认证数据加密技术及单点登陆模型的使用使得越来越多的企业工作平台有了一定的数据安全保障,不仅对企业,对个人也是一种长久且经济有效的数据保护方式。

6 结束语

网络及计算机技术的高速发展为人们的生活工作带来了更多的便捷,创造了更多的可能性,但与此同时信息数据的安全性问题也对企业的成长带来了严酷的考验。如何保证工作平台的信息数据安全成为了一个企业必须去克服的困难问题。而在实际的生活之中,为了保证信息数据的安全,以及降低信息数据泄露对企业造成的直接或间接的经济损失,必须使用一定的数据加密技术手段来确保信息数据安全。

【参考文献】

- [1]王恒,孙从友. 数据加密技术在计算机网络安全中的应用价值分析[J]. 计算机产品与流通, 2019(09):13.
 - [2]江宁. 计算机网络安全中数据加密技术的应用[J]. 电子技术与软件工程, 2019(15):171—172.
 - [3]魏宏. 基于统一身份认证的数据加密技术在网络安全中的应用[J]. 网络安全技术与应用, 2014(01):120—121.
 - [4]于婷. 数据库加密技术在企业信息化管理中的应用分析[J]. 硅谷, 2013, 6(09):115.
- 作者简介:曾垂勇,男,生于1996年,四川泸州人,本科,研究方向:数据加密技术