新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/8/13- 2007/8/19 第38期

网络记录器 / IR系列报导

技术浅谈与应用 - Web IM 的及时监控

随着科技发展迅速，使用网络来传递数据、沟通讯息也越来越便捷，其中最多人使用的沟通管道就是实时通讯（Instant Message，简称 IM）。就是因为其安装简易、使用方便、不需付费...，所以现今全球已有超过 75% 的网络人口在使用实时通讯来做为傳遞文字訊息、檔案、語音與視訊交流的重要途径。

虽然实时通讯使用上如此简单、又不需要付费使用，对于企业来说应该是营销、沟通的极佳利器，但往往也成为员工打混摸鱼的最佳管道。经由实时通讯传送文件文件可能包含病毒、有害程序代码或外泄企业机密，造成企业严重的信息安全风险。就因为实时通讯对企业营运来说像是一把两面刃；可为企业带来丰厚商机，亦有降低员工工作效率的潜在问题。因此，有部分的企业开始采用信息安全设备管制或记录员工使用实时通讯。

这些信息安全设备是针对实时通讯软件的联机特征（Pattern）来阻挡或是记录聊天讯息，让企业可掌握目前常用实时通讯软件之使用状况。但正所谓上有政策，下有对策，实时通讯又不是一定要安装软件方能使用－目前各家实时通讯厂商相继推出了 Web IM（Web Instant Messenger），可以讓使用者透過 Web 介面，使用諸如 MSN、Yahoo...即時通讯服務。Web IM 是采用 HTTP 之方式连接至 Web IM 网页，因而导致一般信息安全设备无法正常阻挡或是记录，造成实时通讯管理上的严重漏洞。

有鉴于此，新软系统在其网络记录器－IR 系列中，加入了 Web IM 分析引擎。透过引擎的分析，IR 系统可明确分辨出哪些 HTTP 联机属于网页浏览、哪些联机属于 Web IM 聊天，再经由 IR 系统内建的记录分析、行为管理两大功能做以下之动作（以 NUS-IR2000 为例）：

记录分析－ NUS-IR2000 目前可记录 MSN 官方的 Web IM 聊天内容。当系统撷取到 Web IM的聊天联机时，NUS-IR2000 内建的记录分析功能会先以使用者为记录之依据，并详细记录聊天双方的账号、昵称、聊天时间、聊天内容...重要信息。管理人员可清楚得知员工于上班时间如何使用Web IM，亦可藉此记录做为日后评鉴考绩之依据。（如图一）

行为管理－ NUS-IR2000 可阻挡员工使用 Web IM，让公司员工无法连结至其服务网页。如此一来，员工仅无法联机至 Web IM，但仍可以正常上网。

图一 可清楚记录 Web MSN 聊天内容

	新软网络记录器	一般市售网络侧录设备
IM	可阻挡与记录聊天内容	可阻挡与记录聊天内容
Web IM	可记录 Web IM MSN Web Messenger（官方）	不可记录数据，甚至无法阻挡
	可阻档 Web IM Buddy. com　Imunitive I Love IM　Wablet Meebo　Gooway IM haha　MSN2go Kool IM　Totmomo messengerFX　Mobile communi　webQQ Mabber	

表一 新软网络记录器与一般市售网络侧录设备之比较表

文 卓冠伦 aaron@nusoft.com.tw

市场行销报导 - 如何有效利用网络记录器的硬盘容量

在企业大量使用网络传输讯息的同时，为了对这些往来的数据把关，市面上出现了许多网络侧录相关产品。这些产品可记录所有员工的网络行为，但所记录之数据却往往都缺乏系统归类或过于草率。导致获得的只是一堆庞大却难以调阅之信息，并无法针对记录特性有效分配储存空间。

有鉴于此，新软网络记录器于研发之初即采用深入撷取、过滤、分析、归纳封包的方式，发展出独特之数据探勘技术。管理人员可针对记录数据内容做全方位检索，实时调阅所需数据。然而，为了详细记录信息来支持“调阅数据的便利性”，新软网络记录器势必需要建置庞大的记录分类数据库。

此时，有人不禁会问，新软网记录器内建硬盘的储存空间，总有使用完毕的时候，难道此时侧录动作就此停摆？为了避免此情形的发生，在新软网络记录器中，管理人员可依企业需求调整各种记录（SMTP、POP3、HTTP、IM、Web SMTP、Web POP3、FTP、TELNET）的保存期限（一般企业会优先保存邮件记录）。新软网络记录器会利用管理人员所设定的保存期限与该服务的实际流量估算各项网络服务之储存空间值，有效分配各类记录于其内建硬盘中的使用率。

新软网络记录器除了使用保存期限方式来确保硬盘之空间外，同时也采用了储存空间临界值预防机制。当新软网络记录器的记录数据，达到设定的保存期限时，即会将其立即清除；若是在数据保存期满前，储存空间就已饱和，新软网络记录器会依照储存数据的历史排序，从目前保留最久的记录开始删除的动作，腾出一定比例的空间，以维持后续侧录动作。

所以，当企业网络环境中，配置了新软网络记录器。在运作一段时间后，即可依照其所计算出来的每日平均流量，和储存数据的重要性，设定记录保存的期限，以制定弹性的空间使用率。

为了因应企业在各法规的实行下，要长时间保留所有往来数据以供查阅的需求；同时防止客户端邮件遗失或误删的情形，则可应用新软网络记录器内建的远程备份机制，将记录数据备份至远程的 NAS、File Server. . .，来确保重要记录可长期保存。

文 程智伟 rayearth@nusoft.com.tw