新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/3/23- 2009/4/5 第88期

网络记录器 / IR系列报导

技术浅谈与应用 - 如何选择网络记录器的三种记录模式？

网络记录器于目前资安设备中，早已经是个不可或缺的重要环节，在林林总总的资安事件不断发生下，相信不少公司企业能够深深了解到资安方面上各项记录是最为重要的凭证依据。举凡讯息传递、实时通讯、电子邮件…等，该如何将其内容一一记录下来当作存证依据？如何避免网络的资源被滥用、泄密及保存公司重要的数据？网络环境越演越复杂，加上网管人力总是不够用的情况下，选择正确的网络侧录设备才能够帮助网络管理者、企业经营者，以最精简的人力及最少的时间下满足记录存证与资安方面的需求。

而这些记录数据如要有完整的证据能力，就需要清楚标示该记录属于哪位员工所有，以下除了将大家所熟悉的 "By IP" 、 "By MAC" 两种模式归纳整理出所适用的时机及需注意之使用情况外，也针对 "By AD Server" 模式做说明，让管理人员能够有效率的为公司选择最适当的记录模式。

By IP Addresses

适用时机：企业网络环境内部的使用 IP 都有固定分配。

注意：因为此种记录基准是以每位使用者的 IP 为判断条件，倘若使用者所使用 IP 可任意作变更，或是所使用的 IP 为浮动式 IP（使用 DHCP）情况下，采用此种模式时较容易发生所记录下的内容不易分辩该项记录 IP 当时为谁所使用，导致误判的情形增加。

By MAC Addresses

适用时机：此模式采用 MAC 为记录基准，可有效避免有心人士任意变换 IP 逃避查缉的问题发生，若企业内部 IP 可由使用者随意变更或不固定时(如：DHCP)皆可适用此模式。

注意：当企业网络内部有架设路由器时要特别注意的是，透过路由器传递的封包其 MAC 会被路由器之 MAC 取代，所以网络记录器的记录基准需要采用以 IP 方式记录，才不会发生路由器后端使用者上网记录错误的情况。

By AD Server

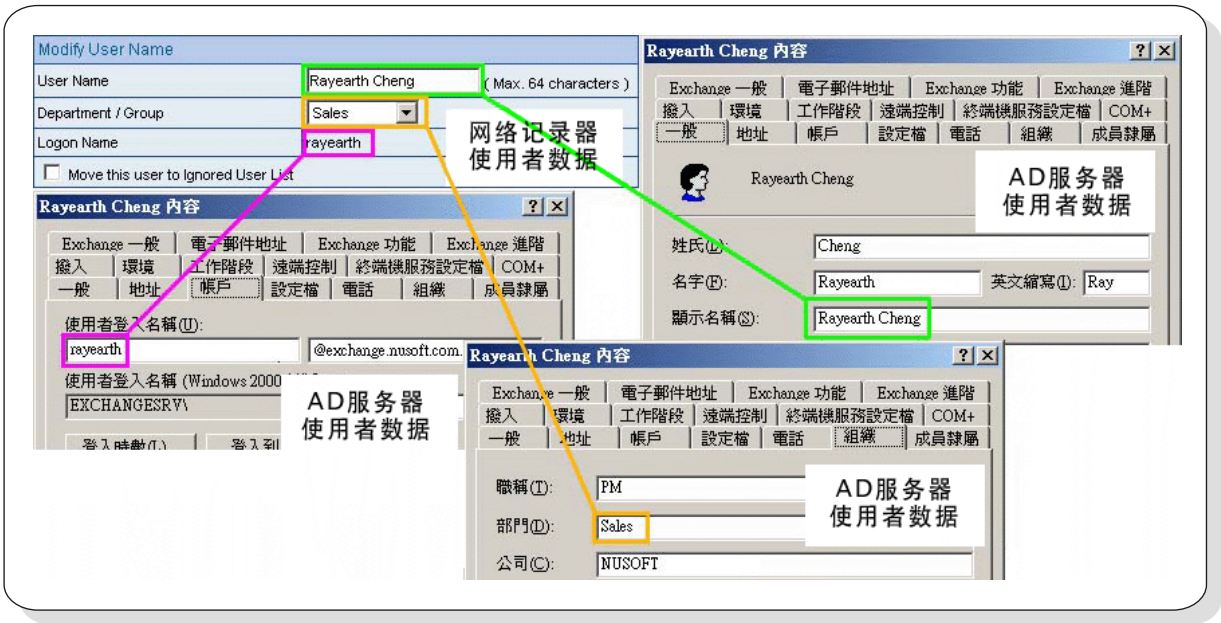
适用时机：企业内部若有架设 AD 网域时。

注意：需搭配系统中所另附之辅助程序 "IR Plug-in" 使用，利用 IR Plug-in 来统整结合 AD Server 上使用者的账号数据。

好处：使用 By AD 模式后，能够有效将其网录记录器之记录依据结合企业内部所辛苦架设的 AD Server，即使是使用者名单有所变动时(如：新进员工、转调部门、员工离职…等)，也只需要更改 AD Server 里面的设定，网络记录器-IR 上的记录就跟着改变，完全不用管理人员再费时于机器设备上调整与变动。同时管理人员不需要再一个一个重新于 IR 中建立名单，在面对公司内使用人数较多情况下即可有效的节省掉不少设定时间与精力上花费。

	By IP	By MAC	By AD
适用环境	有固定分配 IP	IP 无固定分配	有架设 AD Server
注意	使用者可随意变更其使用 IP 或 IP 为不固定（DHCP）时，不建议使用此模式。	若封包之传递有透过路由器时其 MAC 会被路由器之 MAC 取代，所以不建议使用此模式。	需搭配 "IR Plug-in" 结合使用。

记录模式比较表



By AD 模式与 AD Server 结合图示

文 陈殿鸿 kim@nusoft.com.tw

市场行销报导 - IM 实时通讯内容采用「分离式对话视窗」方式记录，让资安管理更方便

在企业 e 化后，因特网系统对企业的营运绩效，有着不可取代的重要性。然而，方便的网络环境，除了能提升营运管理的效率，背后也隐藏着信息应用上的风险，诸如：客户数据的保密、公司机密的泄漏…等等。因此信息安全和管理稽核的结合已经是企业里密不可分的重要管理政策。而方便的 IM 实时通讯工具是目前奔驰商场之重要武器，但是过于方便的使用已成为资安关注焦点。相关研究报告显示，全球约有 30% 以上企业采用 IM 从事商业沟通，却只有少数企业做到 IM 的管控。一方面借着使用 IM 实时通讯而获得便利性的同时，另一方面企业也必须积极运用管理工具来有效管控 IM 的使用。藉以避免发生如:员工趁机摸鱼、公司机密外泄…等状况发生。因此各企业对自己公司内部资安控管产生新的需求，尤其「网络信息监控」、「收集」、「事后查询」等相关需求，俨然成为目前各企业首要解决的重要问题。

而对「IM 实时通讯」做控管的最好方法，首推以「积极开放、有效管理」；依企业的网络政策决定何者方有权限使用实时通讯对外联络，再以网络侧录方式详加记录通讯内容，来替企业信息安全把关。一般网络侧录设备的 IM 聊天记录方式是采用「聊天室」方式记录对话讯息；此种记录方式虽然可以将员工的聊天内容逐条记录，但是若员工同时与两个以上之对象交谈，则易导致聊天内容混杂。使管理人员在事后阅览记录时“很难确定该名员工此时到底是与谁在对话”的情况发生，造成管理上的不易。

因此新软在所推出的「新软网络记录器」系列产品中，特别针对「IM 实时通讯」这部分，采用「对话窗口」模式来分类对话讯息，大大有别于其它市售产品；在其记录表当中，不同对话窗口的聊天内容将分别记录于不同笔记录中。即使员工同时与两个不同对象交谈时，其交谈记录亦不会彼此混杂在一起，管理人员也能够轻易了解所有对话内容。在新软系统的网络记录器里，能使监控对象在记录器下无所遁形，而且其具备便利、科学的检索规则，能大大减少管理者分析记录的时间，让管理工作更方便、更有效率。

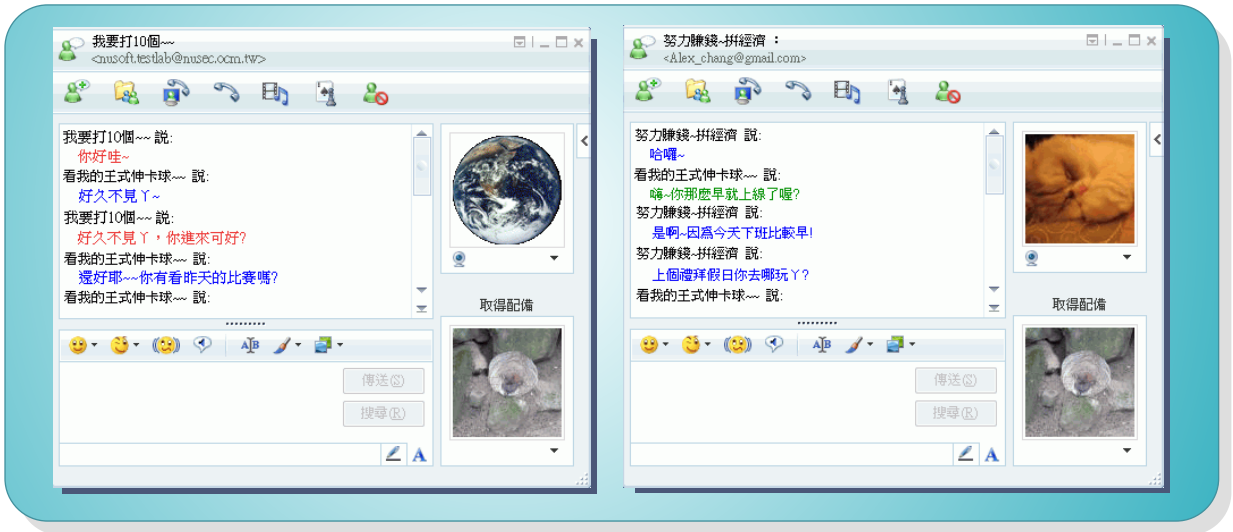


图 1　透过 MSN，员工可同时与多人聊天

图 2　一般网络侧录设备采用“聊天室”方式记录实时通讯，易造成混淆。

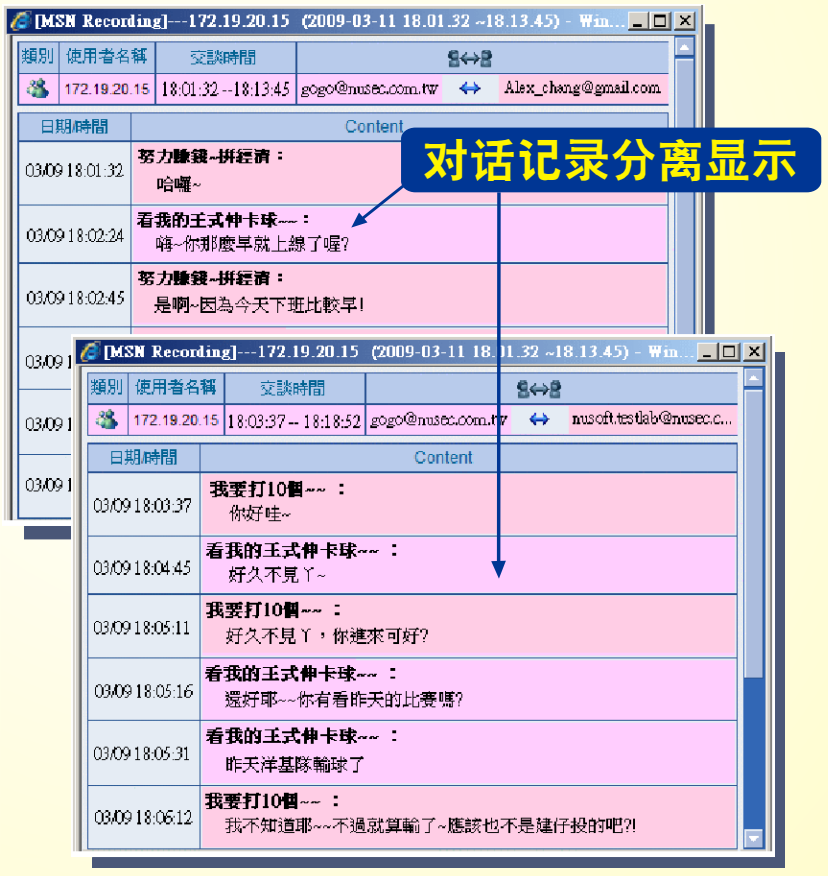


图 3　新软网络记录器的记录采用「分离式对话视窗」记录机制

文 黄政铭 ming@nusoft.com.tw