传统的网络安全只有专业人员才看得懂，普通人常常看不见、摸不着、抓不住——

可视化，给网络安全擦亮眼睛

本报记者 陈莹莹

网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。

习近平总书记今年4月在网络安全和信息化工作座谈会上的这段讲话，被中国科学院信息工程研究所信息安全国家重点实验室主任林东岱在日前召开的全国首届可视化网络安全技术论坛上引用。

“这‘三个不知道’，正是由于网络安全通常看不见、摸不着、抓不住。”林东岱说，解决这“三个不知道”，需要可视化技术。这一技术的本意，便是让网络安全“能感知、可体验、好追溯”。

看得见才是“真安全”

让网络安全看得见，就要建立可视化平台，让不懂安全的人看懂安全、体验安全、维护安全

何为可视化？

“有贼我知道，你倒是抓一个出来看看。我们做网络安全的，最常听到客户这样抱怨。”北京安博通科技股份有限公司CEO苏长君说，安全设备常常买、安全事件常发生、出了事儿一头雾水——客户对于网络安全不可控、不可知，就是因为缺少一个基于安全视角的可视化网络平台。

所谓可视化，就是把网络管理中人员准入、带宽流量等关键信息，以图形化方式展现出来，通过数据、配置、策略、效果的可视，使管理者全面掌握网络状态。

简而言之，可视化针对可疑的流量、数据，目的是让不懂安全的人看懂安全、体验安全、维护安全。

苏长君对可视化的关注，始于一次安博通“内贼”事件。

2014年，安博通遭受了一次网络攻击。一个员工账号总是远程登录，而登录地址又很陌生。“这位员工没有出差，为什么要远程登录呢？”苏长君试着用一些可视化的手段追踪，发现该账号一直在拷贝技术代码，对登录地址做了溯源后，追查到是一家市场上的竞争对手。最终，被证实是一名跳槽去了竞争对手公司的离职员工，仿冒在职员工的账号远程登录。

抓贼经历让苏长君开始反思：传统的网络防护还能适应新时期的安全需要么？

他说，传统的网络安全还大部分停留在网络边界防护、漏洞检测和特征补丁与日志分析上，这些手段都相对孤立和静态，只有专业人员看得懂，客户则很茫然。

打个比方，企业自身的内网与互联网之间有一道门，传统网络安全好比请门卫看守大门。一旦有人带着枪炮前来，就会被门卫拦住。但现在，网络安全开始向着“高级持续潜伏”转变，敌人打入内部，一开始完全不具备“枪炮”特征，就是个正常人，通过很长一段时间，甚至3到5年的潜伏才逐步实现自己的目的。

“当门卫不再能辨别出风险时，最好的方法就是在大楼的每一个角落安装摄像头，每个人访问了什么路径、下载了什么资源、登录了什么网站，都被摄像头一一记录，通过全网可视化盯梢持续性和潜伏性的威胁。”苏长君说。

可视化平台就像是管控一个车站，先划分出不同区域，然后在进站区安装检测仪器、在站内区域和不同位置安装摄像头、重点区域有民警手动核查身份证、售票区域有执法人员打击黄牛、车站周边严防治安问题，共同构成一个防御体系。

最近，安博通与中科院信息工程研究所合作研发的SG-8000系列深度安全网关正式发布，这款采用了多媒体内容安全识别技术的产品，能够广泛应用于国防、公安、平安城市等不同场景。

“我们必须推进国产化战略，在对网络安全起重大作用的信息基础设施和信息关键核心技术方面，实行国产化替代，其中可视化安全领域就是一个重要方面。”中国工程院院士倪光南说，在“互联网+”这一挑战与机遇并存的新时代，信息化已成为全面推动产业升级的支柱力量，而与信息化相辅相成的网络安全，是发展的前提、也是发展的保障。

学老中医治“未病”

治“未病”强调事前安全，增强企业自身的网络免疫能力，将防御模式从被动转为主动

“圣人不治已病治未病，不治已乱治未乱，此之谓也。”郭峰引用了《黄帝内经》中的这句话来阐明自己的观点。

作为太极股份信息安全事业部总经理，郭峰认为，国内的信息安全圈注重攻防多于防御，过分聚焦外部的攻击和威胁，却忽视了企业信息安全自身防御体系情况。

“不治已病治未病，这一理念同样适用信息安全领域，企业对于安全的认识通常是在安全事件发生后，属于事后安全，而‘治未病’强调事前安全，增强企业自身的网络免疫能力，将防御模式从被动转为主动。”郭峰说。

他说，作为行业风向标，全球最具权威的IT研究与顾问咨询公司Gartner公布了关于2016年十大信息安全技术的研究成果，其中自适应体系的核心强调了可视化监控，让可视化在整个信息安全领域中得到了极大的关注。通过提高网络自身免疫力，让业务系统兼具自适应的防御和修复风险的能力，让业务安全可视、可管、可控，是可视化网络安全技术的核心理念。

“就像人体免疫系统随时处于战备状态，一旦有病菌侵入身体，就会迅速发现并作出反应。”苏长君说：“当我们设置好网络基线或策略时，这张网就具备了自身免疫力。”

他解释说，这相当于事先规定一栋大楼哪两道门之间不能走、哪两层楼之间不通、哪些人不能去哪些地方。一旦财务部人员的电脑访问研发部的代码服务器，就好比一个人进了不该进的办公室，可视化系统就会及时响应、触发报警、消灭外部入侵。不但敌人潜伏路径易被发现、内部的安全弱点更易暴露、入侵之后的追踪和取证也容易得多。

“这是智慧城市治理的关键技术。”在首届可视化网络安全技术论坛上，中国电子科技集团首席专家董贵山作出如下判断：基于电子政务，依托可视化技术构建的智慧城市是未来的发展趋势。

他说，通过网络空间本身的可视化，能实现网络治理的可视化；通过信息化，又能在网络空间实现社会治理的可视化。

“在未来智慧城市和网络治理中对接各类数据和应用，这一技术能为城市管理者、城市服务者、公众等智慧城市主体提供直观、科学、全面的数据资源分析结果展示和未来预判，是基于大数据和电子政务实施智慧治理的关键支撑技术，将为智慧城市的构建提供有力的网络安全保障。”董贵山说。

指尖新经济

山东胶州：

O2O提速服务百姓

本报记者 刘 成 通讯员 刘 伟

“自己反映的问题受到重视，并且很快得到了解决，心里感觉像这水一样的甘甜。”山东省胶州市胶西镇尹家店二村村民张秀贞望着清澈的水流说：“现在村民们遇到问题，打开手机、动动手指，就可以享受到快捷便利的服务。”

原来，由于连续的干旱，前些天尹家店二村出现了吃水困难现象，部分村民在“微服万家”微信公众号上进行了留言，希望镇政府帮忙解决。

接到群众的诉求后，镇分管负责人王书满立即组织相关部门到村庄进行了实地调研，摸排出群众的实际需求和当地的水文地质情况。通过讨论研究，最终决定投资14万元，在村委会附近挖凿一个100米深的水井，并结合三级提水安装净化设备一套，免费向村民开放。

“以前，群众惯性的诉求表达方式渠道单一，往往局限于找村干部、镇干部，认准一个人、认定一件事，却时常‘找不到人’或‘找不对人’。”尹家店二村党支部书记王山家认为，“微服万家”解决了传统处理群众诉求“周期长、速度慢、效率低”的问题。

“微服万家”微信服务平台是胶西镇运用手机微信软件，创新打造的“线上服务键对键，线下服务面对面”O2O服务模式。平台一站式受理、办理群众诉求，实现了数据多流动、部门多跑步、群众少走路。记者登录平台看到，“微服万家”公众号由胶西发布、胶西党建和便民服务三大板块组成，群众可以随时随地了解相关政策、咨询相关事项、进行网上留言，有任何诉求都可以第一时间以文字、图片等形式通过公众号上传至服务后台。

对于群众的具体诉求，常规性问题立即填写纸质阅办单，交由责任部门予以办理；涉及情况复杂的综合性问题，则由镇党委书记亲自部署，部门联动解决。同时，微信公共服务平台限定48小时用户响应时效，办结的事项会及时反馈给问题提报人，并对办理结果进行实地督查考核和群众满意度回访，确保群众反映的事项事事有回音、件件有落实。

此外，胶西镇专门设置了“微服万家”接办员、专办员和督办员，全镇机关干部以“微服专员”身份对接联系全镇114个村庄和近400家企业，全镇663名组织网格员负责收集、解决、督办群众诉求，为民服务24小时不打烊。“村里都贴有‘微服万家’二维码，村民只要拿起手机扫一扫，就可以添加关注，及时了解政务动态、反映相关诉求。”张秀贞说。

“微服万家”的应用，将原先的线下办理转为线上办理，领导在线上直接批办，职能部门在线上直接领办，办理结果在线上直接反馈给群众，群众不仅仅能看到办理结果，还能看到事项的整个办理流程，真正实现了无纸化办公，大大提高了工作效率。

“为方便群众使用微信，减少流量成本，辖区内已实现无线WIFI全覆盖。”王书满介绍说，“微服万家”开通以来，已受理群众诉求556件，办结率99.3%，群众满意度99.7%，解决群众诉求的时效由原来的4个工作日变为4个小时，甚至是即知即办。

在线餐饮看好二三线城市

本报讯 记者王金虎报道：近日，“乙丁快餐”项目在山东省泰安市正式上线运营。“眼下，在线餐饮的用户和商户大量在一线城市聚集，一线城市覆盖率达到84.1%；二三线城市虽然占比较小，但迅猛发展。”乙丁公司董事长关海祥认为，经过几年发展，在线餐饮在一线大城市的渗透率接近饱和，下一步，发展渠道应向二三线城市下沉，二三线城市的人们生活成本较低，压力较小，更愿意享受在线餐饮的便捷。可以预见，二三线城市将是下一轮竞争的主战场。

食品的安全卫生是送餐APP存在的隐患。针对此，“乙丁快餐”通过技术创新，让消费者在浏览餐品的同时，可以通过手机APP看到整个中央厨房24小时360度无死角的实时监控视频，并且在餐品配送过程中还能以地图的形式查看配送人员的即时位置。“我们的目标是打造让管理者省心、加工者用心、消费者放心的在线餐饮平台。”关海祥表示。

国家认监委信息中心与阿里巴巴合力建“云桥”——

大数据护航“有机认证”

8月17日清晨，新疆赛里木湖上，捕鱼船缓缓张网作业，赛湖渔业的工作人员小心翼翼地将生长在深达90米冷水中的高白鲑打捞上来。

同在船上的还有国家认证认可监督管理委员会和第三方有机食品认证机构的工作人员。他们不断作记录，通过采集水样，严密检查高白鲑的生长环境等，以确定其是否达到有机产品认证标准。如果通过，其公司的产品将会被打上“有机认证”标识，出现在阿里巴巴平台上。

对于不少吃货来说，好消息是，美味的高白鲑即将从遥远的新疆赛里木湖来到淘宝。这背后是阿里巴巴与国家认监委信息中心借助大数据实现的有机产品溯源与保真机制。

近日，阿里巴巴与国家认监委信息中心完成“有机产品认证”数据对接测试，这使得国家认监委遍布全国的认证机构的实地检查结果能迅速同步到电商平台，实现政府、电商平台、社会第三方机构大数据多元共治。

赛湖渔业是一家省级农业龙头企业，其主打产品高白鲑生长在海拔2100米的新疆赛里木湖中，全年产量300吨左右，因而成为有机认证的热门产品。

像后者一样正在进行认证并打标的产品还有很多，目前仅淘宝平台就已有400余件商品完成了有机认证和地理标志产品打标。其中既有与地方政府合作，引入防伪技术实现对五常大米的全程追溯，又有“政府认定、协会推荐、平台管控”阳澄湖大闸蟹的互联网+传统水产行业模式，但贯穿始终的都是大数据。

在认证现场，国家认监委信息中心有关负责人李锋告诉记者，认监委掌握着大量的产品认证认可等数据，目前正在搭建“云桥”平台，将这些数据进一步开放给公众，由于电商平台能够直接触达终端消费者，认监委加强与相关电商平台的合作是一个重要方向。

国家认监委“云桥”平台从去年12月底已经建设，首先和阿里巴巴建立了3C数据的对接，今后将进一步开展有机认证的数据合作。

据介绍，“云桥”本身就是数据对接的平台，通过顶层的数据接口来实现政府数据面向社会的广泛共享，把认证的结果和表达的信任传递出去。“我们也需要这些平台去核查存在问题的产品，并反馈给我们，来实现社会监督和行政监督的联动，探索整个市场的多元共治的机制。”李锋说。

而消费者的反馈数据正是电商平台的强项。阿里巴巴平台治理部商品管理中心负责人袁征说，接入数据以后，在阿里巴巴平台上产生的销售、服务、品控等数据也会反向形成预警，比如《有机产品认证证书》明确标注了经认证产品的产量、生产规模，一旦销售超过认证产品总量，监管机构将在线下采取行动；比如利用大数据绘制商品品质地图，成为执法部门开展线下精准打击的线索。

“不久前，3C认证数据的对接已取得很好的效果，现在已经在做监控测试了，而有机数据对接的调试也已经有5个月了。”袁征说，认证已经形成了数据回流的机制，通过大数据把可能有问题的商品反馈给监管部门，相应的监管部分和认证机构会根据反馈的数据到线下去落实认证，这才能真正形成一个线上线下互动的机制：线上商家商品有问题可以对商家商品作处理，线下可以到源头上去对制造商进行检查，形成一个闭环。

据介绍，阿里巴巴不断接入多个政府部门权威数据，以期实现对商品质量的更好管控。袁征称，尽管重视度在提升，但其平台上十几亿种的商品不可能人工地逐一核实，在打击假冒伪劣商品时平台也并没有线下执法能力，这需要和政府更紧密的配合：一方面在顶层开展批量化的数据对接，传达给消费者；另一方面，利用大数据开展线上线下的执法对接，实现政府、平台、商家、消费者多元共治的社会化治理机制。

文/农 兴

“互联网+西藏文化旅游体验馆”开馆

8月18日，“互联网+西藏文化旅游体验馆”在拉萨众创空间正式开馆。人们既可以通过电子设备用“万能视角”观赏羊卓雍错美景，又可以在手机上体验全方位的阿里风光……体验馆通过前沿的互联网技术使人们与西藏旅游和文化“亲密接触”。图为一名女士在VR体验区戴上VR眼镜体验西藏美景。

新华社记者 张汝锋摄

本版编辑 来 洁