**背景需求**

近些年来，随着互联网技术的发展以及电子商务和电子政务的普及，各企事业单位、党政机关面临的网站安全问题也随之凸显出来。为了继续发挥互联网经济产生效益和优势，需要我们必须积极应对网站安全问题。

目前，国内安全形势非常严峻，网站面临的安全问题大量涌现。首先，网站系统需要应对和处置的安全隐患持续增长，需要企业和机构进一步加强隐患的管理和控制。据CNCERT发布的《2015年中国互联网网络安全报告》显示，2015年CNVD共收录了安全漏洞8080个，其中高危漏洞收录数量高达2909个，该数字较2014年增长21.5%。其次，网站安全事故频发，据CNCERT发布的《2015年中国互联网网络安全报告》显示，2015年，CNCERT/CC共接收境内/外报告的网络安全事件126916起，平均每天发生安全事件347起，数量非常惊人，其中有24550个网站被篡改，40782个境内主机被植入木马或僵尸程序。最后，与网站相关的重大安全事故也频频发生，国内外各知名企业相继发生数起重大安全事故。其中，京东商城泄露12G用户数据、雅虎泄露5亿用户资料、LinkedIn旗下的在线学习网站Lynda.com被窃取950万账号信息等事件都直接导致公众个人信息的泄露。

与此同时，国家对网站安全问题越来越重视，并且不断加大网站安全的监管力度。中央网络安全和信息化领导小组成立后，发布的第一个文件就是《关于加强党政机关网站安全管理的通知》，该文就各级党政机关及企事业单位开展网站安全管理提出若干条指导意见。另一方面，国家各级主管部门加大检查力度，近几年多次开展重要保障活动及安全专项检查工作，并且每次重要保障任务和专项检查工作的重点都包括对互联网网站检测和治理。

**问题和困难**

当前，各党政机关及企事业单位在网站安全管理上存在的问题主要集中在网站的资产管理、漏洞管理、威胁管理、事件管理四个方面。

在资产管理方面，问题主要体现在企业缺乏有效的手段对网站等资产的变更进行监测和管理，导致新上线的网站或变更的网站在未经安全检查和采取防护措施的前提下直接暴露在互联网上。通常这些网站存在大量安全隐患，非常容易被攻击者所利用。

在漏洞管理方面，企业所面临的困难主要是未能对网站漏洞及隐患进行定期排查和处置，导致未发现、未处置的漏洞数量越来越多。通常有两方面原因导致漏洞数量的增加，一方面是用户网站内容变更可能会引入的新漏洞，另一方面是先前网站建设过程中引入的第三方代码会被不断发现存在新漏洞。

在威胁管理方面，企业面临的主要问题在于缺乏专职人员对安全防护设备及其防护策略进行维护，使得安全设备检测效能逐步降低。效能降低主要体现在两个方面，一方面是监测和防护新威胁的安全策略不能及时得到应用；另外一方面是网站业务系统的不断变更导致原先的防护规则逐步失效。

在事件管理方面，企业面临的主要问题是缺乏有效手段及时发现安全事故，使得安全事故造成影响和损失不断增加。

**方案介绍**

绿盟网站安全监测与防护解决方案能够通过事前漏洞分析与预防、事中威胁监测与防护、事后安全事件监测与响应，迎接国家合规检查、抵御外部威胁、降低安全风险。

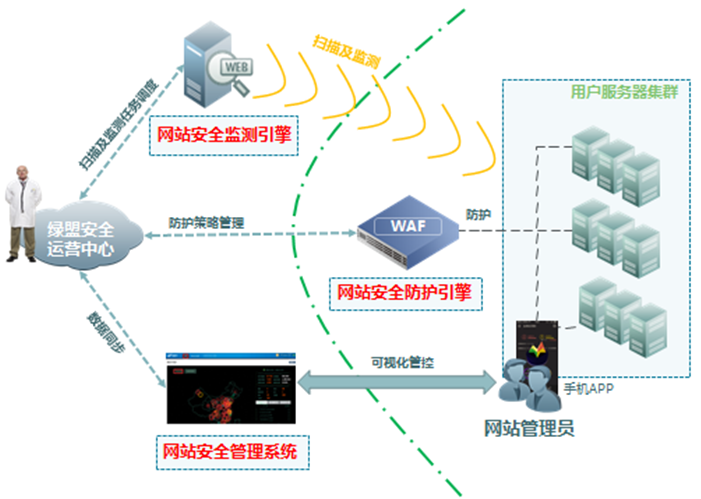


图1：绿盟网站安全监测与防护解决方案

绿盟网站安全监测与防护解决方案，主要由网站安全管理系统、网站安全监测引擎以及网站安全防护引擎构成。网站安全管理系统能够为用户提供在线的、可视化的管理工具，帮助用户查看和处置网站安全相关的资产事件、漏洞事件、威胁事件和安全事故。网站安全监测引擎可以帮助用户监测网站变更的情况、网站存在安全漏洞以及发生的安全事故。网站安全防护引擎采用绿盟Web应用防火墙产品，部署在用户侧，用于各类web应用攻击的检测和阻断。

绿盟网站安全监测与防护解决方案是通过以下方式来帮助用户完成网站的资产管理、漏洞管理、威胁管理以及事件管理。

在资产管理方面，绿盟网站安全监测与防护解决方案主要通过监测引擎为指定的IP网段进行资产扫描，通过与现有资产比对发现新上线的网站及变更的网站系统，并及时向用户通告。在用户确认资产变更内容后，更新现有资产列表并将变更的资产纳入到安全监测与防护体系中，以便及时发现漏洞、威胁及事故。

在漏洞管理方面，主要通过网站安全监测引擎进行定期漏洞扫描，对暴露在公网上的所有网站进行Web漏洞及系统漏洞扫描工作。此后，由自动化验证系统对于扫描发现的高中危漏洞进行漏洞验证，将具有危害性的高中危漏洞信息通过网站安全管理系统和漏洞扫描报告直接推送用户，用户可以根据各类交付物中所罗列的漏洞详情以及解决方案进行漏洞的整改加固。如果Web漏洞修复周期较长，用户还可以通过网站安全管理系统委托绿盟进行漏洞预防工作。对于修复的漏洞，用户可以通过网站安全管理系统委托完成漏洞复验的工作，从而完成整个漏洞生命周期的闭环管理。

在威胁管理方面，绿盟网站安全监测与防护方案通过安全防护引擎进行威胁防护。防护引擎通过与绿盟云的对接，可以定期对告警日志进行分析判断，并提供筛除误报的策略优化建议。另外，绿盟云也会提醒用户对防护引擎的知识库进行升级，以确保防护引擎可以对新型威胁进行防护。

在事件管理方面，通过网站安全监测引擎对目标网站进行安全事故的日常监测，确保能够在第一时间发现网站挂马、篡改、黑链、敏感内容、可用性通断等多方面问题。在发现事件后，通过短信、网站安全管理系统及手机APP等多种方式第一时间向用户告警。另一方面用户可通过网站安全管理系统委托绿盟通过网站安全防护引擎消除安全事件造成的影响。最后，绿盟本地应急响应工程师上门协助用户分析事件原因，找到导致事件发生的根源，并提供加固建议和支持，消除存在的安全隐患。

**方案优势**

       绿盟网站安全监测与防护解决方案的六大核心优势：

提供7\*24小时的全天候服务，发现安全问题后确保30分钟内通知用户。

支持托管模式，0维护成本。

所有事件经过自动化技术和安全专家验证，准确率接近100%。

提供短信、邮件、网站安全管理系统、手机APP等多元化通告方式，确保及时进行通告。

为用户提供漏洞智能补丁，对修复周期较长的漏洞提供预防措施。

通过网站安全管理系统，提供漏洞风险、威胁攻击、灾害事故可视化展示，让用户一目了然的洞悉全单位风险、攻击及灾害分布。



图2：网站安全管理系统

**方案实践**

截至2016年，已监测等保二级以上的网站数量累计达21516个，商业客户数量近1000余名，客户群覆盖国有银行、股份制银行、国内三大运营商、石油石化企业及电力行业。

2015、2016连续两年承担公安部网站安全专项检查工作，同时支撑并参与了抗战胜利70周年纪念活动安保工作、第二届世界互联网大会安保工作、以及2016年“两会”期间网络和信息安保工作。