U.S. Election Commission Cyber Hygiene Report

A Broader Picture of Election Security

As is painfully aware to election observers, everyone is talking about the safety and security of U.S. election infrastructure. Just ahead of the 2018 midterm elections, Jim Condos, President of the National Association of Secretaries of State (NASS) and also the serving Vermont Secretary of State (SOS), discussed election systems cybersecurity. In a USA Today opinion editorial, Condos indicated he believed most states did a good job – in relation to ensuring elections are secure from hacking – in 2016.[1] While his analysis covers good cyber hygiene and maintenance practices, in retrospect the focus of the practices covered in his article was very narrow. However, Condos has determined that a lot of the internal infrastructure assets at the state election commissions and Secretaries of State offices are relatively safe, but we need to look beyond internal networks to really understand the state of our election infrastructure.

This Normshield report focuses on the broader picture, the internet facing infrastructure that supports state election processes. We have undertaken this review of states' election infrastructure using the approach recommended by the Center for Internet Security (CIS) Handbook for Elections Infrastructure Security. Page 6 of the Handbook states, "The IT systems infrastructure that supports our elections processes has myriad risks, and these risks vary from one organization to the next." On page 8, CIS identifies three classes of elections systems. This report focuses on the first class, Network Connected Systems and Components that are exposed on the internet.[2] We did not review the use of, nor the cyber hygiene for, voting machines; nor does the scope of this report include county voting infrastructure.

The Genesis of the Election Commission Cyber Hygiene Project

NormShield's believes that it has a responsibility to give back to the community as a whole. For example, we offer free community services and search tools that allow consumers to find out if personal credentials have been leaked, or if their web asset(s) are on any IT blacklist. NormShield can then determine if that information or other assets are freely available.

As community members, we are naturally concerned about the safety of our election process and the potential for disruption of its integrity. We noticed, as demonstrated by Secretary Condos' report, that states may be focusing on their internal assets and may not be examining

[1] Condos, Jim. *Ahead of midterm elections, states are working diligently to protect your votes.* USA Today. October 19, 2018.

[2] A Handbook for Elections Infrastructure Security. Center for Internet Security (CIS). V1.0. February 2018. https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf

their broader cyber ecosystem footprint. So, we undertook the exercise of examining that broader footprint to better understand what election system integrity looks like from that perspective.

As a business, we help our customers evaluate the cyber hygiene of their ecosystem using publicly available and Open Source Intelligence (OSInt), which is of course also available to hackers. NormShield collects the available OSInt, determines the digital footprint of an entity, including the entire cyber infrastructure that supports that entity. Next, we analyze that data, correlating findings to reveal where a potential hacker might focus their efforts to compromise that cyber ecosystem. This process is examined in greater depth further on in the methodology section of this report.

We reviewed the available data on election commissions in July 2019, more than a year away from the next general election. We looked at data from all 50 states, the District of Columbia, and five U.S. territories. While we found that many of the commissions are doing very well in securing their systems, there are still a number that are lacking in their overall cyber infrastructure. We then re-examined that data again in August 2019 and have summarized the findings from both inquiries in this report.

Election Commission Notifications

NormShield privately provided its findings to the Secretaries of State (SOS) and election commissions in July in order to empower them with the information needed to remediate vulnerabilities. NormShield ran a second scan in August and found significant improvement in the security posture of several election commissions.

Report Methodology

Thinking and Seeing Like a Hacker

The cyber ecosystem covers a broad range of assets and processes from which a hacker will select a target and undertake reconnaissance on that target, looking for weaknesses. When low-value targets do not provide easy access points, the hacker will simply move on to a different target. High-value targets, however, will be worth more effort; and the hacker will be more persistent in their scrutiny, allowing them to find alternative pathways into the asset.

The 2013 breach of retailer Target is an enduring example of this method of striking through a low value asset to gain access to higher value assets. That large and significant hack of payments information was accomplished through a third-party – Target's heating and air conditioning (HVAC) vendor. Access was gained by hacking the HVAC login and then locating a pivot access point into Target's network. From that access point, jumps were made several times into other networks, until the development area was reached, where access to credentials was discovered that allowed the hack to occur into the payments data. In such significant breaches, it has been shown that 60% of those breaches occur through third-party access points.

This is relevant for election infrastructure concerns, because while the Secretary of State office and election infrastructure may be secure, each SOS and election commission also consumes (outsources) services from third parties. This outsourcing exposes the election infrastructure to a potential breach in which a hacker could pivot into an election system through a third-party access point.

Standards-Based Scoring

NormShield's grading methodology follows and applies a well-known and commonly-used Cyber Threat Susceptibility Assessment (CTSA) and Common Weakness Risk Analysis Framework (CWRAF™), both developed by the MITRE Corporation in partnership with the U.S. Air Force. CTSA and CWRAF provide a framework for scoring software weaknesses in a consistent, flexible, open manner, while accommodating context for various types of business operations. Normshield's grading assesses the risks vis-a-vis CTSA and CWRAF and converts that risk into rankings and easy-to-relate-to letter grades. Information security practitioners find these methods facilitate their ability to quickly identify and prioritize risks.

The benefits of using CTSA and CWRAF:

- Provides mechanisms for measuring risk of any security errors ("weaknesses") that are mission or business critical.
- Supports the automatic selection and prioritization of relevant weaknesses, customized to the specific needs of the organization's business or mission.
- Uses the Common Weakness Scoring System (CWSS™) to identify the most important weaknesses for relevant business domains, in order to inform acquisition and protection activities as one part of the larger process of achieving software assurance.

100+ Assessments

There are 100+ items that the scorecard checks during these assessments. Examples of the items can be found in the addendum to this report. We map each finding to a related Common Attack Pattern Enumeration and Classification (CAPEC™) and Common Weakness Enumeration (CWE), both of which are created by MITRE. CAPEC is an effort that provides a publicly available catalog of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities.[3] CWE is a community-developed formal list of common software weaknesses. It serves as a common language for describing software security weaknesses; a standard measuring stick for software security tools targeting these vulnerabilities; and a baseline standard for weakness identification, mitigation, and prevention efforts.[4]

[3] The Mitre Corporation. https://capec.mitre.org/about/index.html

[4] The Mitre Corporation. https://cwe.mitre.org/about/index.html

For example, if we find a Use of a Broken or Risky Cryptographic Algorithm (SSLv3 or v2), we use CWE-327 (Use of a Broken or Risky Cryptographic Algorithm), CWE-693 (Protection Mechanism Failure) and CWE-719 (OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage) to define the weakness in a standard language. Moreover, we also use CAPEC-223 (Employ Probabilistic Techniques), CAPEC-20 (Encryption Brute Forcing) and CAPEC-97 (Cryptanalysis) to describe the possible attack techniques in a standard classification.

Data and Findings

July Scan

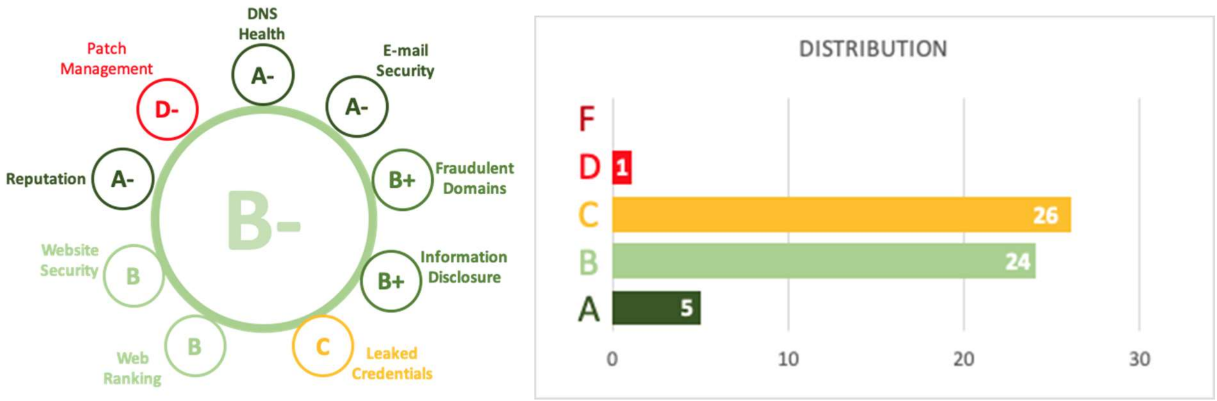

Figure 1: Overview of Initial Findings

Category grades

The cybersecurity posture of an organization can be assessed from different perspectives. An organization’s cyber hygiene may look good overall; however, categorization helps to determine where it does look weak. In reviewing why more than half of the commissions received a grade C or below, Patch Management was the category where most did poorly. This is mainly because of the use of outdated systems.

Table 1: Overview of Category Grades

	Number of Commissions with a certain grade				
Category	A	B	C	D	F
Patch Management	22	4	12	5	13
Website Security	6	28	21	1	0
Leaked Credentials	36	3	2	8	7
Fraudulent Domains	36	8	12	0	0
E-mail Security	41	4	9	2	0
Information Disclosure	45	0	11	0	0
IP/Domain Reputation	45	6	1	4	0
DNS Health	41	12	2	1	0
Web Ranking	41	12	2	1	0

Use of outdated systems

Hackers try to exploit the vulnerabilities on systems, especially if the system is outdated. Outdated systems require very strict patch management policies. Intuitively, up-to-date systems have fewer vulnerabilities. When we look at the most used services by the election commissions, we found that more than half use Windows Server 2008 r2 and Microsoft IIS 7.5 where Windows Server 2019 and Microsoft IIS 10.0 are available. We can even see that some Election Commissions use Windows Server 2003.

Windows 2003 is an example of a legacy system that is no longer supported by its manufacturer. DHS Cyber+Infrastructure (CISA) sent out an alert that Windows 2003 would no longer be supported by Microsoft, including for automatic fixes, updates, or online technical assistance. CISA listed among the impacts: “Computer systems running unsupported software are exposed to an elevated risk to cybersecurity dangers, such as malicious attacks or electronic data loss.” and “Organizations that are governed by regulatory obligations may find they are no longer able to satisfy compliance requirements while running Windows Server 2003.”[5] Microsoft has announced that it will end support of Windows 2008 on January 14, 2020, well ahead of the 2020 election cycle.[6]

[5] Alert (TA14-310A): Microsoft Ending Support for Windows Server 2003 Operating System. DHS CISA. November 10, 2014. https://www.us-cert.gov/ncas/alerts/TA14-310A

[6] Microsoft Announcement. Microsoft Corporation. Retrieved 2019 from: https://www.microsoft.com/en-us/cloud-platform/windows-server-2008

Table 2: Overview of Systems Use by Server Type

Most Used Services	
Service with version numbers	Number of commissions using the service
windows server 2008 r2	32
microsoft iis/7.5	28
windows server 2012 r2	23
windows server 2016	11
microsoft iis/8.0	6
nginx/1.10.2	5
nginx/1.14.0	5
apache/2.2.15	4
microsoft iis/6.0	4
windows server 2003	4

Old Systems Creating New Attack Vectors

Attack vectors are magnified in these situations, in part due to the combination of:

- failure by most organizations to monitor Internet of Things (IoT) devices;
- coupled with flat networks and a lack of network segmentation (a compliance must); and
- the additive factors of a general lack of inventories for identifying network assets (including IoT devices)[7] or preventing shadow IT because of a lack of Network Access Control (NAC).

Every organization, industry vertical, and government has to contend with the presence of IoT, which ranges from WiFi printers, monitors, and security alarms to HVAC control sensing devices. And IoT devices that are uncontrolled can cause serious compliance issues, policy violations, security incidents, and loss of life or safety issues in manufacturing and operational technology (OT) environments. In relation to election security, we discovered the use of outdated systems was prolific with 56% of commission's still using Windows 2008 servers and another 40% using Windows 2012 servers along with old versions of Microsoft Internet Information Services (IIS). Common exploitable issues we found most prevalent in nearly 70% of commissions included missing DMARC records, missing glue records, and invalid or expired SSL certificates. Nearly 31% of commissions already have a compromised asset which has been reported and blacklisted.

[7] Third Party IoT Risk: Companies Don't Know What They Don't Know. The Shared Assessments Program & Protiviti, Inc. 2019; The Internet of Things (IoT): A New Era in Third Party Risk. The Shared Assessments Program & Protiviti, Inc. 2018. https://sharedassessments.org/studies/

Susceptibility to Phishing is Magnified

The most common issue that we have discovered is the missing DMARC Record. DMARC Records are essential to prevent spoofing attacks through email. Hackers can send emails that look like the emails are coming from a legitimate organization. A DMARC record (along with SPF record) can prevent that from happening. Thirty-nine commissions had missing DMARC records.

More than 40% of the election commissions have at least one website with an invalid or expired SSL certificate. Adversaries can leverage this lack of security by penetrating the websites.

Table 3: Overview of Issues and Number of Commissions where the Issue was Present

Issue	Severity (out of 10)	Number of commissions with the issue
Missing DMARC Record	4.7	39
Missing Glue Records	3.9	28
SSL Certificate Invalid, Incorrect, Expired, or Self-Signed	6.4	24
Sensitive Cookie in HTTPS Session without Secure Attribute	4.0	15
Data Breach Index	7.2	12
Missing SPF Record	4.7	11
Lack of DNS Subnet Redundancy	5.5	6
Missing Domain A Records	5.3	6
Lack of SMTPS Connection (TCP-25)	5.6	6
Cross-Site Request Forgery (CSRF)	6.5	4

Risks for Botnet and Spam Attacks

If a digital asset of an organization becomes a part of botnet or spam propagation, the organization’s IP addresses are listed in publicly available blacklists. Almost one-third of the election commissions have at least one asset that is reported by blacklist databases.

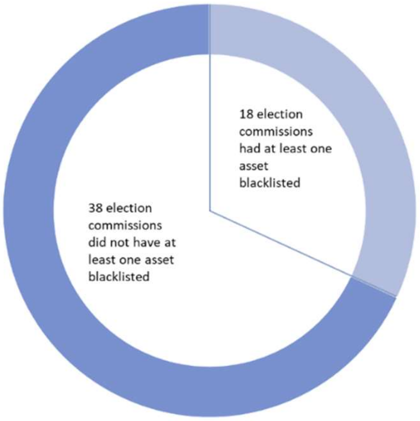

Figure 2: Percent of Commissions with Blacklisted IP Addresses

Conclusions and Recommendations

The overview from our investigation gives us insight into how the commissions look in regard to their information technology and securing their platforms.

With 56% of commissions using 2008 Windows Servers, those commissions represent the weak prey in the herd – the easy target for the predator. The rest of the herd protecting that weak member is the information security team providing compensating controls to mitigate the presence of old servers. The commissions seem to have come to the conclusion that their security team efforts will keep the servers safe. That may have been true in the past, but today we have a new and different group of predators seeking weak targets. Ten years ago, it was just one wolf that had to be outrun. Now there are thousands of predators and the weak beast will surely fall to at least one of them.

So why do commissions fail to upgrade their servers in order to eliminate this vulnerability? The costs associated with performing those upgrades certainly stand in their way. Costs in this case are both financial and technical. While it is problematic for commissions to allocate the relatively significant financial and human resources required to mediate this problem, they also face a technical system problem. The programs that are used to provide services to the citizenry of each state, district, and territory are technically designed to operate on that older platform (in this case Windows 2008). An upgrade may break the functionality for service provision across the platform. Resolving this issue is significantly more complex. Solving this problem would require upgrading all the applications that live in that environment. So far, commissions have attempted to keep their systems secure by applying compensating controls. That would be sufficient, if the hackers were all of lower skill levels than the information security staff designing and applying those solutions. However, that is not the case. The hacker often reaches its target – the wolf often gets its prey.

When we conducted our initial review of the commissions' election cyber ecosystem, we notified all the commissions, territories, and the District of Columbia and made the results, as well as access to a full remediation database available.

Improvements in August

We conducted a follow-up review thirty days after our initial review. We are happy to report that we have seen a major improvement across the board. One state had a D- and was next to last in the rankings in the first scan. That state has improved two full grades and moved up in ranking 16 spots. Fifteen states improved their score from C to B. The average score improvement was 2%, while one state in particular improved its score by 17%. These improvements were achieved by updating services and remediation of most common issues. For example, the ratio of election commissions with the top common issue, missing DMARC Record, dropped from 69% to 59%.

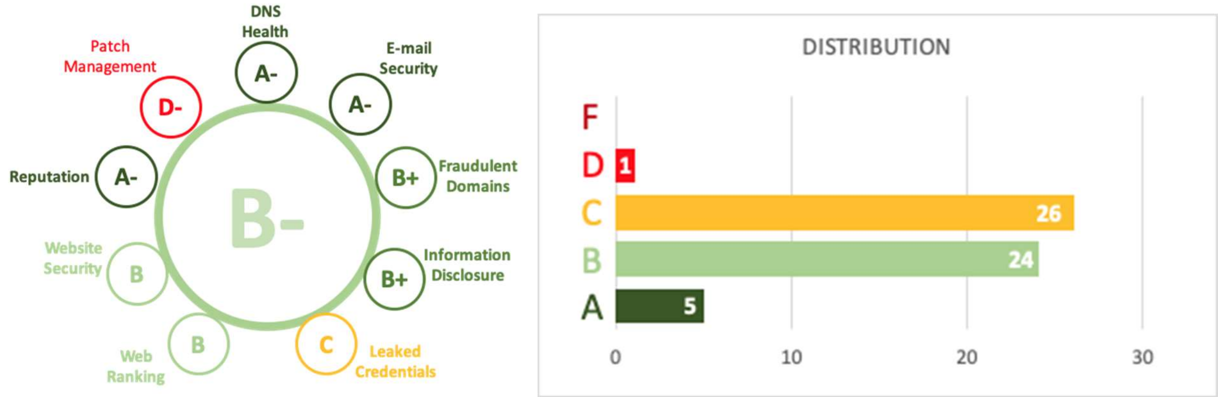

Figure 3: Overview of Initial July Findings

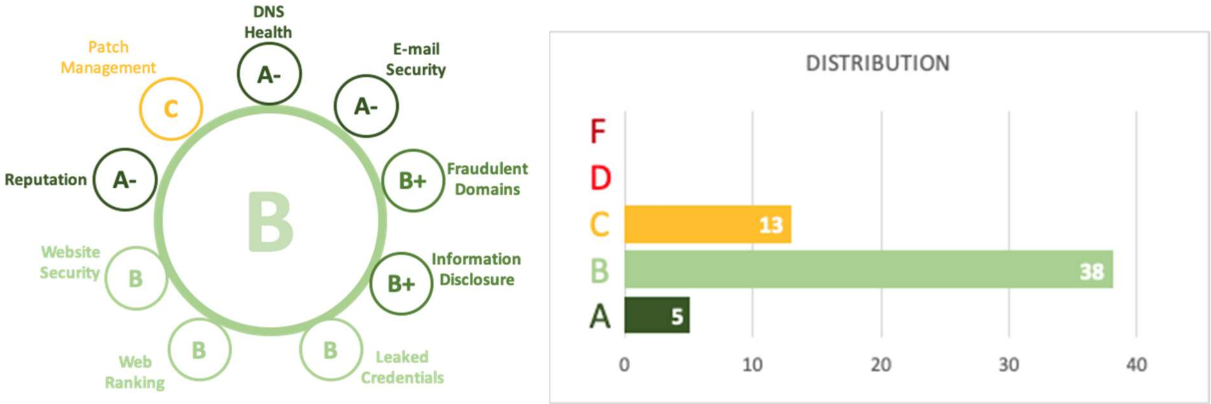

Figure 4: Overview of Updated August Findings

Our recommendation to resolve this problem is two-fold. In the short term, vulnerabilities and potential attack vectors have to be monitored on a real-time basis on systems that present the highest risk and addressed as they are discovered (also real-time). In the long term, our political leaders need to understand the complexity of the IT systems that have been put in place to provide services for our citizens, and they have to be willing (exert the political will) to financially support CISOs and SOSs with improved staff and infrastructure resources.

States must become more aware of their cyber ecosystem footprint. As with other types of operations, "The core problem is poor risk measurement leading to poor prioritization of security efforts."[8] States must improve their working understanding of what systems truly represent the most risk. Risk is not just present at the level of the Secretary of State's website; all of the underlying supporting infrastructure (and third-party services supporting that infrastructure) must be taken into account, evaluated, and the associated risks must be mitigated as well.

[8] *Capital One Breach Shows Cybersecurity Is "Lost in Noise", Jack Jones Tells New York Times*. FAIR Institute Blog. August 1, 2019.
https://www.fairinstitute.org/blog/capital-one-breach-shows-cybersecurity-is-lost-in-noise-jack-jones-tells-new-york-times?utm_content=97781101&utm_medium=social&utm_source=linkedin&hss_channel=lis-HvCIsYFwIz

However, this effort still falls short of protecting election system assets. In addition to building awareness, critical infrastructure must be upgraded, patched, and replaced to give our elections the best opportunity to remain free and secure.

As Intelligence Chairman Richard Burr (R-N.C.) stated, “In 2016, the U.S. was unprepared at all levels of government for a concerted attack from a determined foreign adversary on our election infrastructure.” He gave credit to states, municipalities, and the Department of Homeland Security (DHS) for working actively since the 2016 election to “bridge gaps in information sharing and shore up vulnerabilities.” Burr also stated that “There is still much work that remains to be done, however. It is my hope that the Senate Intelligence Committee’s bipartisan report will provide the American people with valuable insight into the election security threats still facing our nation and the ways we can address them."[9]

[9] Mitashak, M. Senate Intelligence report on Russian meddling sounds alarm for 2020. Politico. July 25, 2019. https://www.politico.com/story/2019/07/25/russia-interference-2016-election-1435436

Addendum

Table 4: Sample of Scorecard Check Items Showing Mapping between CAPEC and CWE

Control	Description	Related CAPEC IDs	Related CWE IDs
DNS Cache Snooping	DNS cache snooping is a technique that can be employed for different purposes by those seeking to benefit from knowledge of what queries have been made of a recursive DNS server by its clients. Uses of this information vary, ranging from planning which mis-typed domains are worth registering (for marketing and other purposes) through to determining which domains might be easiest to target for a cache poisoning attack.	598 148	16
Open Recursive Name Server	Open Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks. DNS resolvers that allow queries from all IP addresses and are exposed to the Internet can be attacked and used to conduct Denial of Service (DoS) attacks on behalf of the hacker.	607	923
Open DNS Zone Transfer	DNS zone transfer, also sometimes known by the inducing DNS query type AXFR, is a type of DNS transaction. A zone transfer that from an external IP address is used as part of an attacker's reconnaissance phase. Usually a zone transfer is a normal operation between primary and secondary DNS servers in order to synchronize the records for a domain. This is typically not something you want to be externally accessible. If an attacker can gather all your DNS records, they can use those to select targets for exploitation.	291	862
SPF Record	An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of your domain. The purpose of an SPF record is to prevent spammers from sending messages with forged From addresses at your domain.	163 98	353
DMARC Record	Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email-validation system designed to detect and prevent email spoofing. It is intended to combat certain techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations.	163 98	353
DKIM Record	Domain Keys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing. It allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain.	163 98	353
SSL Certificate Invalid, Expired or Self-Signed	SSL protocol makes sure that user information travels safely through the Internet in a secure manner if the certificate is trusted. This helps prevent an evil-intentioned attacker from sniffing the network to steal confidential information like users' credentials	156 459	295 290
Heartbleed (CVE-2014-0160)	Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited regardless of whether the party is using a vulnerable OpenSSL instance for TLS as a server or a client.	546 97	126 693
Use of a Broken or Risky Cryptographic Algorithm (SSLv3 or v2)	SSL and TLS are cryptographic protocols designed to provide communication security over the Internet. SSLv2 was quickly found to be insecure. SSLv3 was created, and, recently Google engineers pointed out that SSLv3 is broken (with an exploitation technique known as POODLE) and should not be used any longer.	223 20 97	327 693 719

Application Level Weaknesses (20+ controls)	Vulnerabilities and weaknesses related to web applications create risks for the users of these web applications. Login forms without encryption, lack of bot detection or missing web application best practices can be exploited by hackers to bypass authorization and authentication of company resources. Insecure web applications allow attackers to access confidential information. Hackers usually use this confidential information to leverage their attack vector or sell it in underground markets.	574	200
Cleartext Transmission of Sensitive Information	Failure to encrypt sensitive communications means that an attacker who can sniff traffic from the network will be able to access the conversation, including any credentials or sensitive information transmitted. Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications. Encryption (usually SSL) must be used for all authenticated connections, especially Internet-accessible web pages, but backend connections as well.	157 389	311
Information Disclosure	Information disclosure is when an application fails to properly protect sensitive information from parties that are not supposed to have access to such information in normal circumstances. These types of issues are not exploitable in most cases. However, they are considered as security issues because they allow attackers to gather information which can be used later in the attack lifecycle, in order to achieve more than they could if they didn't get access to such information.	163	200
Server Version Disclosure	"Server" header tells the web server software being run by the site. Revealing the specific software version of the server may allow the server machine to become more vulnerable to attacks against software that is known to contain security holes. [RFC 2068]	574 580 170	200
Transport Layer Protection	The primary benefit of transport layer security is the protection of web application data from unauthorized disclosure and modification when it is transmitted between clients (web browsers) and the web application server, and between the web application server and back end and other non-browser based enterprise components. Failure to encrypt communications means that an attacker who can sniff traffic from the network will be able to access the conversation. Encryption (usually SSL) must be used for all authenticated connections, especially Internet-accessible web pages, but backend connections as well.	102 158 383	319
Possible Fraudulent Domains	Fraudulent domains and subdomains are used to run phishing campaigns by attackers. The attacker registers a domain with a name similar to the target company. Attacker can develop a web site using the logo, design, or any other content that actually belongs to a company and can share this web site on the internet. Then, the attacker can phish the customers by redirecting them to malicious domain via a link.	163 543	254 358
IP Reputation	Blacklists contain lists of IPs or domains that pose a threat to consumers. Asset reputation lists the IPs or domains that are blacklisted or that are used for sophisticated APT attacks. The reputation feeds are collected from VirusTotal, Cymon, Firehol, BlackList DNS servers, etc.	548	254 358
Web Ranking	The web applications are the public face of all businesses. Well optimized, high performance websites are most desirable for most of internet users. If the content of the website is not compatible with best practices it may not properly rendered on many browsers. Lack of user interaction and experience impact the website visibility and business success ratio.	548	254 358