National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

CURRENT PROJECTS

We guide U.S. businesses to stronger cybersecurity practices

USE CASES

CONSUMER/RETAIL SECTOR

Multifactor Authentication for e-Commerce

E-commerce fraud impacts consumers, retailers, payment processors, banks, and card issuers, but retailers often bear the cost for fraudulent transactions. An increased level of assurance in purchaser or user identity can help reduce this risk. This project will demonstrate how retailers can implement stronger authentication mechanisms in card-not-present scenarios (e-commerce transactions) through multifactor authentication tied to existing web analytics and contextual risk calculation.

Securing Non-Credit Card, Sensitive Consumer Data

Retailers can gather consumer data during typical business activities to accelerate business operations and revenue, including date of birth, address, phone number, email address, and purchasing habits. There has been an increase in the value of this data on the black market, and relatively few regulations or standards exist to combat it. This project will help retailers better secure non-credit card, sensitive consumer data through data masking, tokenization, and fine-grained access control.

ENERGY SECTOR

Identity and Access Management for Electric Utilities

Many utilities run decentralized identity and access management (IdAM) systems managed by numerous separate departments. This creates inefficiency and can result in security risks for utilities. The NIST Cybersecurity Practice Guide, *Identity and Access Management for Electric Utilities*, demonstrates an example converged IdAM platform that can provide a comprehensive view of all users and their access rights across the enterprise.

Situational Awareness

To improve the security of information and operational technology, including industrial control systems, energy companies need mechanisms to capture, transmit, analyze, and store real-time or near-real-time data from these networks and systems. This project explores methods by which energy providers can detect, remediate, and investigate anomalous conditions and share findings with other energy companies.

FINANCIAL SERVICES SECTOR

Access Rights Management

Identity and access systems employed by the financial services sector are often fragmented and operate in isolation from one another, creating vulnerabilities that allow exploitation by attackers and insider threats. This project aims to enable financial services sector entities to centrally issue, validate, modify, or revoke access rights for an entire enterprise.

IT Asset Management

Security professionals in the financial services sector are challenged by the vast diversity of hardware and software they attempt to track as well as a lack of centralized control. The NIST Cybersecurity Practice Guide, *IT Asset Management*, details an example comprehensive IT Asset Management (ITAM) system that allows financial services organizations to centrally monitor and gain deeper insight into their entire IT asset portfolio using an automated platform.

HEALTH IT SECTOR

Securing Electronic Health Records on Mobile Devices

When health information is stolen, inappropriately made public, or altered, health care organizations can face penalties, lose consumer trust, and patient care and safety may be compromised. The NIST Cybersecurity Practice Guide, *Securing Electronic Health Records on Mobile Devices*, demonstrates a platform to securely document, maintain, and exchange electronic patient information among mobile devices.

Wireless Infusion Pumps

Security breaches on wireless infusion pumps that deliver fluids, medication, or nutrients to a patient's circulatory system or gastrointestinal tract can harm the patient through incorrect dosing or compromised protected health information. This project will identify the risks of network-enabled infusion pumps, and provide an example security solution.

LEARN MORE ABOUT NCCOE
Visit http://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

BUILDING BLOCKS

Attribute-Based Access Control

Access to a company's network and assets is usually defined by a user's job or role within a company, using a Role-Based Access Control system. If roles change or an employee leaves the company, an administrator must manually change access rights accordingly, oftentimes within several systems. The NIST Cybersecurity Practice Guide, *Attribute-Based Access Control*, provides an example solution using granular attributes such as title, division, certifications, and even environmental conditions to authorize user access.

Data Integrity

Data Integrity can alter or destroy critical information such as customer data, transaction records, and correspondence. The NCCoE data integrity project will explore methods to effectively recover operating systems, databases, user files, applications, and software/system configurations from malicious attacks. To address real-world business challenges around data integrity, the resulting example solution will be composed of open-source and commercially available components.

Derived PIV Credentials

To gain access to federal information systems, the current standard requires a two-factor authentication consisting of a Personal Identity Verification (PIV) enabled smart card and a password. While larger devices such as desktop and laptop computers easily facilitate the use of a smart card, the newer generation of computing devices such as tablets, convertible computers, and mobile devices present significant challenges. This project will demonstrate how derived smart card credentials can be added to mobile devices so that they can be used for remote authentication to information technology systems in operational environments.

DNS-Based Secure Email

Organizations need to protect their server-based email security mechanisms against intrusion and man-in-the-middle attacks during the automated cryptographic service negotiation process. Consequences of such breaches can range from exposure of sensitive or private information to enabling fraudulent activity by an attacker posing as the victimized user and disabling or destroying the user's system—or that of the user's parent organization. This project will demonstrate a security platform that provides trustworthy mail-server-to-mail-server email exchanges across organizational boundaries.

Mobile Device Security: Cloud & Hybrid Builds

Mobile devices allow employees to access information resources anywhere at any time. If sensitive data is stored on a poorly secured mobile device that is lost or stolen, an attacker may be able to gain unauthorized access to that data. The NIST Cybersecurity Practice Guide, *Mobile Device Security: Cloud & Hybrid Builds*, demonstrates how businesses can use commercially available technologies to implement an enterprise mobility management system. These technologies enable users to work inside and outside the corporate network with a securely configured mobile device while minimizing the impact on the user experience.

Privacy-Enhanced Identity Federation

While the benefits of federated identity management are significant for both organizations and individuals, these connections can create new cybersecurity and privacy concerns. Both organizations and users must be able to trust that the federated identity management service is not going to reveal sensitive information during participation. The primary goal of this project is to demonstrate how federated identity services, leveraging market-dominant standards, can include privacy enhancements directly in the solution.

Software Asset Management Continuous Monitoring

To support decision-making and automated action to reduce enterprise risk, security officers need accurate, timely information about the current state of software installed, authorized, and used on computing devices. This project will demonstrate software asset management capabilities that include precise data collection and the secure exchange of software inventory data from devices. This functionality may be used as part of a larger continuous monitoring capability that supports basic situational awareness of the software installed and in use on monitored devices.

Trusted Geolocation in the Cloud

Shared cloud computing can generate security and privacy challenges. Companies also expose themselves to legal, policy, and regulatory risks when workloads are migrated from cloud servers in one country to servers in another. This project uses an automated "hardware root of trust" to determine the integrity of the computer hardware and restrict workloads to cloud servers within a location. The hardware root of trust is a tamper-proof combination of hardware and firmware with a unique identifier for the cloud server host and metadata about the server platform. Businesses can access this information via secure protocols to find out if the platform is as it was when first deployed, the location of the cloud server, and to enforce geolocation-based restrictions.

HOW TO PARTICIPATE

We are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you are interested in contributing or collaborating on these projects to enhance the nation's ability to recover from data integrity attacks, please contact us at: nccoe@nist.gov. Learn more about the projects at https://nccoe.nist.gov/projects.