GIRITECH®

Deutschland · Österreich · Schweiz

ZeroTrust

Vielschichtige IT Security

IT Security stellt sich als eine vielschichtige Aufgabe dar. Zum einen gilt es die verschiedenen Teilaspekte einer sorgfältigen Betrachtung und Risikobewertung zu unterziehen, zum anderen bedeutet IT Security mehr als die Installation technischer Instanzen.

Letztlich geht es um vermeiden und verhindern, Verantwortung und Vorbereitung.

Vermeiden und verhindern.

Die Internet Polizei warnt: *„Vermeiden Sie den Besuch unsicherer Webseiten, Downloads fremder Dateien und Klicks auf Links mit unbekanntem Ziel“!*

Dieses zugegebenermassen leicht humoristische Intro verdeutlicht das Dilemma.

1.) **Anwender sind keine digitalen Firewalls. Wie sollen sie verantwortlich und verlässlich entscheiden welche Aktivitäten erforderlich und gewollt sind und welche risikobehaftet?**
Natürlich ist ein hohes Maß an Sensibilisierung erforderlich. Aber die heutigen Cyberangriffe sind bei weitem ausgeklügelter als in den Anfangszeiten. Professionelle Phishing E-Mails lassen sich nicht mehr einfach anhand ihrer abenteuerlichen Rechtschreibung identifizieren. Gefährliche Webseiten sind professionell gestaltet und der jeweilige Content der zu der gewünschten Interaktion führen soll ist oft hinreichend plausibel.

2.) **Digitalisierung ohne verstärkte Durchdringung Internet gestützter Services schliesst sich aus.** Wenn aber grosse Bereiche der Business-Ökosysteme mit Schnittstellen zu Lieferanten, Kunden, Transaktionsportalen interoperieren steigt das Risiko einer Kompromittierung – oft mit „durchschlagender“ Wirkung.

Wie sieht eine Vermeidungsstrategie aus?

Ziel ist nicht die Nutzung zu vermeiden, sondern die damit verbundenen potentiellen Gefährdungen zu eliminieren. Dabei betrachten wir folgende Teilaspekte:

Netzwerk Access Security
Wer oder was erhält direkten kabelgebundenen oder kabellosen Zugang in unser Intranet?

Remote Access Security
Wie stellen wir sicher dass unser - im Zuge zunehmender remote Zugänge erheblich erweiterter - Perimeter nicht zur breiten Angriffsfläche wird?

Endpoint Security
Welche Maßnahmen schützen den Endpoint dergestalt, dass Kompromittierungen ausgeschlossen werden und damit keine Einfallstore für Schadsoftware entsteht?

Internet Security
Wodurch wird surfen im Netz sicher?

NAC, Network Access Control

Network Access Control (NAC) ist die Zugangskontrolle für kabelgebundene und kabellose Endgeräte in die jeweiligen LAN Infrastruktur. Der Standard IEEE 802.1x beschreibt ein sicheres, portbasierenes Authentifizierungsverfahren.

Die Authentifizierung erfolgt über Zertifikate, Benutzerkonten oder MAC Adressen. Zertifikate stehen dabei für den höchsten Sicherheitslevel – MAC Adressen für den niedrigsten. Allerdings befinden sich in vielen Netzen noch Endgeräte mit älteren Betriebssystemen die eine „strong authentication“ nicht unterstützen. (Beispielsweise Steuerungsrechner, medizinische Devices u.a.)

Damit wird erreicht, dass kein unbekanntes Endgerät per physischer Anschlussdose oder WLan Zugang ins Netz der Organisation erhält. Authentifizierte Teilnehmer werden automatisch in die ihnen zugewiesenen VLAN Segmente getagged. Accounting Funktionen regeln wann Benutzer Zugang erhalten und ob Benutzer mit mehreren Geräten angemeldet sein dürfen.

Ergänzend unterstützt NAC eine verschlüsselte WLan Kommunikation. Zertifikate vermeiden zudem Probleme die durch veröffentlichte pre-shared keys (PSK) entstehen können.

Remote Access Security

Viele Organisationen und Unternehmen verlassen sich traditionell auf Virtual Private Networks (VPN) Instanzen um Fernzugriffe bereitzustellen. VPN-Verbindungen wurden jedoch originär dafür konzipiert Site-to-Site Verbindungen (also Standort Vernetzungen) einzurichten. Werden hingegen aktuelle Anforderungen (Home Office, allgemeine mobile Zugriffe) durch VPN Anbindungen erfüllt, geht dies mit einer teils erheblichen Anzahl Site-to-End Verbindungen einher. Dabei wird der Netzwerk Perimeter um diese Vielzahl externer, unüberwachter Knoten erweitert.

Netzwerksicherheit wird damit zu einer großen Herausforderung. Angreifer können, sobald sie über kompromittierte Clients Zugriff auf ein VPN erhalten, in das Unternehmensnetzwerk eindringen und dort ihre schädliche Wirkung entfalten. Ungeachtet der Notwendigkeit externe und mobile Zugänge bereitzustellen ist es unverzichtbar das zentrale Netzwerk und die externen Devices vor den damit verbundenen erhöhten Risiken zu schützen. Dies wird zu einer besonderen Herausforderung, wenn die externen Geräte nicht der Kontrolle des Unternehmens unterliegen – also unter die Kategorie ungemanagt und untrusted fallen.

Die Alternative heisst virtual Access. Virtual Access vermeidet aufgrund seiner Architektur die mit VPN verbundenen Probleme und Schwachstellen da der Client nach erfolgreicher 2-Faktor / Multifaktor Authentifizierung zu keinem Zeitpunkt direkten Zugang ins Zielnetz erhält und der remote Zugriff ausschliesslich auf explizit freigegebene Anwendungen / Desktops möglich ist.

Endpoint Security

Angriffe gegen den Endpoint sind vielschichtig. Das Ziel besteht letztlich darin den Endpoint zu kompromittieren und mit den so übernommenen Benutzerrechten entsprechende schädliche Operationen durchzuführen. Dabei ist Ransomware prominentester Vertreter dieses Genres – aber Cyberangriffe sind oft subtiler und weitreichender.

Z. B. kann sich ein Angreifer durch sogenanntes „lateral Movement“ im Unternehmensnetz bewegen und sich Kenntnisse über interne Abläufe, Kundendaten, Zugangsdaten etc. verschaffen und die gewonnenen Informationen gezielt zu einem späteren Zeitpunkt für einen Cyberangriff zu nutzen.

Bezüglich „Daten als neue Währung“ gilt dass beispielsweise von Gesundheitseinrichtungen entwendete Daten um ein Vielfaches teurer gehandelt werden als Kreditkarteninformationen.

Eines haben alle Angriffe gegen Endpunkte gemeinsam. Jede Malware basiert letztlich auf ausführbarem Code - es muss ein Prozess gestartet werden, der die Malware wirksam werden lässt. Ein möglicher Lösungsweg zur Vermeidung besteht in einer konsequent angewendeten Ausführungs- und Prozesskontrolle. Mehrstufige Endpoint Security beinhaltet einen zentral gemanagten Antivirenschutz, einer Geräteport Überwachung, einer Positivliste freigegebener Anwendungen und gegebenenfalls einem Integritätsschutz der für einen gesicherten, normierten Systemzustand sorgt.

Moderne Lösungen sind als Cloudangebote verfügbar die eine zentrale Sicherheitsadministration der Endgeräte ermöglichen, Aktualisierungen / Patches am Endpoint initiieren sowie Warnmeldungen und Reports erstellen.

Internet Security

Der Browser ist die weltweit meistgenutzte Anwendung. Praktisch jedes intelligente Endgerät verfügt über einen Browser, immer mehr Anwendungen nutzen den Browser als Kommunikationselement. Aktive Inhalte sorgen für hohen Komfort und unterstützen Anwender dabei, verschiedenste Prozesse automatisiert auszulösen. Allerdings beinhaltet diese wachsende Browser Nutzung Sicherheitsrisiken.

Laut Data Breach Investigations Report[1] ist die Zahl der Cyberangriffe 2021 um 13 Prozent gestiegen, Google notiert bis zu 30.000 neue Webseiten mit bösartigem Schadcode pro Tag.
Anwender erkennen in der Regel nicht, auf wie viele externe Javascripts, Domains, iFrames und mehr eine Internetseite nach dem Öffnen zugreift und möglicherweise kompromittierten oder unerwünschten Code auf dem Endpunkt ausführt.

Schutz bietet Remote Browser Isolation. RBI verlagert die Ausführung von Website-Code weg vom Endpunkt. Malware kann damit kein Angriffspotenzial mehr entfalten. Ransomware- und Phishing-Attacken werden ebenso wirkungsvoll blockiert wie Zero-Day-Malware.

[1] https://www.lanline.de/it-security/ransomware-gefahr-eskaliert.254366.html

Web-Apps, browserbasierter Zugriff und damit verbundene Risiken

Vier primäre Datenexfiltrationswege vor denen sich Unternehmen schützen müssen.

Datendiebstahl und Unternehmensspionage sind nur einen Klick entfernt, da vertrauliche Daten über den Browser ganz einfach auf persönliche Webspeicherkonten übertragen werden können.

Cloud-Speicherlösungen machen es Benutzern leicht, Bilder und Daten von jedem Gerät aus zu speichern. Benutzer können Unternehmensdaten durch ein einfaches Drag-and-Drop in ihrem eigenen, persönlichen Cloud-Speicher ablegen.

Für Benutzer die zu schnell die Auswahl „Tab schließen“ betätigen, sind Browser-Caches die Rettung. Ein erneutes öffnen des geschlossenen Tabs bringt verlorene Daten zurück.

Kommt das Device abhanden oder wird gehackt ist es jedoch problematisch, wenn vertrauliche Daten aus Web- oder Cloud-SaaS-Anwendungen noch im Cache des Devices sind. Umso mehr, wenn das Gerät nicht verwaltet wird und die IT keine Möglichkeit hat, Daten - einschließlich Webbrowserdaten – auf dem Device remote zu löschen.

Soziale Medien sind ein wichtiges Marketing Instrument und zur Imagepflege. Andererseits macht die Leichtigkeit des Veröffentlichens Social-Media-Kanäle auch riskant. Benutzer können vertrauliche Daten oder Bilder teilen, ohne zu berücksichtigen, dass die von ihnen geteilten Elemente nur für den internen Gebrauch bestimmt sind – oder deren Veröffentlichung sogar beabsichtigen.

Clevere Social-Engineering-Taktiken verleiten dazu Inhalte zu teilen, die für Angriffe auf ihre Organisationen verwendet werden könnten.

Kopieren ist einfach. Sei es der Ausdruck in eine PDF Datei, das schnelle kopieren der Bildschirmanzeige mittels einem einfachen [Strg]+[P] oder [Alt]+[Druck] Befehls oder die Übertragung von Dateiinhalten über das Clipboard.

Wertvolle Daten aus unternehmensinternen Web- und Cloud-Apps können so unbemerkt zum Schaden des Unternehmens exfiltriert werden.

Bis zur Offenlegung vertraulicher Informationen oder entsprechender Lösegeldforderungen ist es dann oft nur noch ein kleiner Schritt.

Neben den technischen Maßnahmen ist eine wichtige Aufgabe die Sensibilisierung der Mitarbeiter und Mitarbeiterinnen. Dabei gilt es folgende Aspekte zu berücksichtigen:

1.) Welche Regelwerke gelten für ungewöhnliche Anweisungen seitens der Geschäftsführung / des Managements.
Beispielsweise im Umgang mit aussergewöhnlichen Zahlungsanweisungen.

2.) Welche Regeln gelten bezüglich einer allgemeinen Internetnutzung:
(Verbotene Privatnutzung, verbotene Kategorien …)

3.) Was gilt für den Umgang mit unbekannten E-Mail Absendern, eingebundenen Links und E-Mail Attachements, wenn das Unternehmen keine explizite Schutzsoftware einsetzt[(2)]

4.) Welche Verhaltensregeln gelten, wenn in Folge Stress, Flüchtigkeit o. ä. ein Fehler unterlaufen ist? Eine „Angstkultur“ ist in diesem Zusammenhang äusserst kontraproduktiv.

5.) Die Angriffsvektoren ändern sich, werden intelligenter. Daher ist ein permanenter Refresh sinnvoll, der auch exemplarisch bestimmte Szenarien und Abläufe darstellt.

Der „Faktor Mensch“ ist eine wichtige Komponente im Zusammenhang mit Cyber Security – aber er kann und darf Unternehmen und Organisationen nicht dazu verleiten die Verantwortung für sichere IT Nutzung auf die Anwender zu verlagern. Menschen machen Fehler, Mitarbeiter und Mitarbeiterinnen haben in der Regel andere Aufgaben und sind nicht als IT Security Spezialisten ausgebildet.

Trotz aller getroffener Maßnahmen bleibt das Restrisiko Opfer eines wie auch immer gearteten Cyberangriffs zu werden. Daher ist es unerlässlich für diesen Worst-Case eine entsprechende Vorsorge zu betreiben.

Hierzu ist die Erstellung eines Notfallplans, der u.a. folgende Aspekte beinhaltet, unverzichtbar.

- was sind die „unternehmenskritischen Anwendungen“ und wie können diese wiederhergestellt werden (gestaffeltes Restore Konzept)
- Bestimmung von Ansprechpartnern, Vertretern, Aufgaben und Kommunikationswegen
- Interne Krisenkommunikation (Bestandteil der Mitarbeiterunterweisung)
- Externe Krisenkommunikation (Medien, Lieferkette, Kunden)
- Gesetzliche Auflagen / Meldewesen (Beachtung von Fristen)
- Externe Kontaktdaten (Polizei, Cyberversicherung, Forensik, IT-Dienstleister)

[(2)] Beispielsweise die Lösung NoSpam Proxy des deutschen Herstellers Net At Work GmbH

Giritech GmbH bietet folgende Lösungen im Kontext IT-Security:

NAC	: Soliton NetAttest
Secure Remote Access (no VPN)	: Soliton G/On, Ericom Connect
Endpoint Security	: Faronics DF Cloud-Ultimate
Secure Internet	: Ericom RBI