ORT, DATUM

Schule:
Schulnummer:

NUTZUNGSVEREINBARUNG

BRING YOUR OWN DEVICE (BYOD) der SchülerInnen im pädagogischen Netz, ausschließlich gültig für die Nikolaus-August-Otto-Schule & die Pestalozzischule

Mit meiner Unterschrift bestätige ich verbindlich, folgende Hinweise zur Nutzung meines privaten Endgerätes zur Kenntnis genommen zu haben und mich mit Ihnen ausdrücklich **einverstanden** zu erklären:

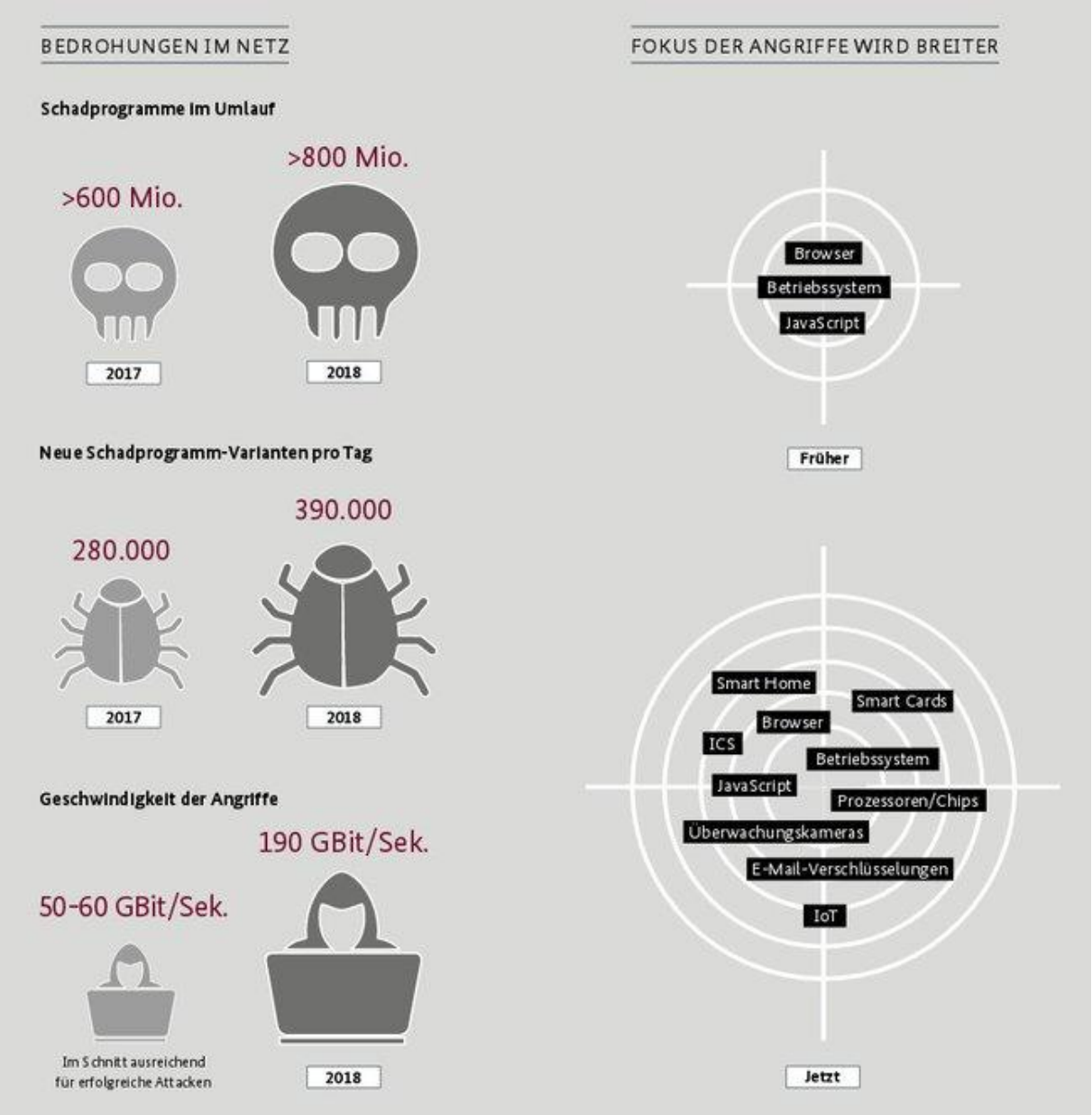
1. In dem sicheren IServ-Netzwerk der Schule dürfen nur vorab über dieses Dokument registrierte, private SchülerInnen-Endgeräte genutzt werden, die zwingend für den Unterricht benötigt werden.

2. Die Benutzung erfolgt auf eigenes Risiko. Für Schäden, die an einem Privatgerät durch einen IT-Sicherheitsvorfall (z.B. Verschlüsselung von Daten; Diebstahl privater Aufnahmen usw.) entstehen, übernehmen Schulleitung und Schulträger keinerlei Haftung.

3. Die Registrierung des privaten Geräts erfolgt nur mit Zustimmung (Unterschrift) der Schulleitung und unter Meldung an den Fachdienst II.9 des Schulträgers RTK. Das unterzeichnete Dokument ist für die Dauer der Einbindung des Privatgeräts in das Schulnetzwerk abzuspeichern / vorzuhalten.

4. Das private Unterrichtsgerät erhält über die personalisierten Benutzerdaten Zugriff auf das IServ-Netz. Mittels Proxy wird der Ausstieg ins Internet über einen sicheren Internetfilter erzwungen. Um dies zu gewährleisten, muss die Schülerin/der Schüler manuell eine einmalige Einrichtung gemäß der beigelegten Erklärung durchführen. (Proxy akzeptieren und eintragen)

5. PRIVATUMGANG
   Das private Gerät muss stets mit einem aktuellen Virenscanner/Malwareschutz betrieben werden (Landesvorgabe). Darüber hinaus ist ein angemessen sicherer Zugangsschutz (starkes Passwort) sowie ein umsichtiges, sicherheitsorientiertes Vorgehen in öffentlichen, ungesicherten Netzen (z.B. WLAN bei McDonalds) und bei potenziell risikobehafteten Internetseiten (z.B. Pickdumps) sicherzustellen. Dies gilt auch für vernetzte Geräte im Internet of Things (IoT).



Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Der Download eines Virus oder Trojaners kann dabei weitreichende Folgen haben. Bestenfalls erhalten die Betroffenen unliebsame Werbung, schlimmstenfalls entstehen hohe finanzielle oder emotionale Schäden. Das Spektrum der Straftaten infolge einer Malware-Infektion ist äußerst groß – Ausspähung, Mobbing, Schaden an IT, Online-Diebstahl, erpresserische Verschlüsselung von Daten, Betrug, Datenverlust, Identitätsdiebstahl oder Verleumdung.

Weitere Informationen des BSI zum Schutz des Privatgeräts und Herausforderungen der IT-Sicherheit für VerbraucherInnen finden Sie hier: https://www.bsi.bund.de/dok/6596708

6. Die Logins ins sichere IServ-Netz werden im Rahmen der gesetzlichen Bestimmungen protokolliert. Aufgerufene Internetseiten o.ä. werden nicht getrackt.

7. Im Falle eines begründeten Missbrauchsverdachts sowie im Rahmen eines konkreten IT-Sicherheitsvorfalls kann jedoch über die rechtskonform erfolgte Sicherung und im Rahmen der gesetzlichen Bestimmungen anhand der Protokolle festgestellt werden, welches Gerät den Vorfall herbeigeführt hat.

8. Bei konkreten Rechtsverletzungen sowie fahrlässig verursachten Risiken durch Verstöße gegen diese Nutzungsvereinbarung (z.B. keine Aktualisierung des Virenschutzes) kann der Verursacher haftbar gemacht werden.

Mit meiner Unterschrift bestätige ich verbindlich, folgende Vorgaben bei der Nutzung meines privaten Endgerätes einzuhalten:

1. Das von mir gemeldete Gerät wird zwingend für den Unterrichtseinsatz benötigt und ich verpflichte mich zu einem verantwortungsvollen Umgang mit dem Schulnetz.

2. Mein Privatgerät ist mit einem aktuellen Virenschutz geschützt und wird in regelmäßigen Abständen auf Malware überprüft. Der Virenschutz wird min. einmal im Jahr geprüft und aktualisiert.

3. Ich verpflichte mich zur Nutzung eines sicheren Passworts sowie einem umsichtigen, sicherheitsorientierten Verhalten in öffentlichen Netzen und auf Internetseiten sowie beim Download von Materialien und Öffnen von E-Mails. Mir ist bewusst, dass dies auch für verbundene Geräte gilt.

4. Ich führe die vorgegebene, manuelle Einrichtung des Proxy durch.

Art des Geräts/Herstellername/Typ	
Klarname SchülerIn	
Unterschrift SchülerIn	
Unterschrift Erziehungsberechtige(r) bei minderjährigen SchülerInnen	

Die Schulleitung erklärt sich mit der Aufnahme des Geräts einverstanden.

Klarname Schulleitung	
Unterschrift Schulleitung Stempel	

Informationen zur Einrichtung des Proxy

Die manuelle Einrichtung des Proxy lässt sich leicht und in der Variante 1 sogar automatisiert bewältigen. Sollten Sie Unterstützung benötigen, wenden Sie sich bitte an die/den IT-Beauftragte/n Ihrer Schule.

Variante 1:

Automatische Proxy-Konfigurations-URL (Empfehlung)

Bitte geben Sie folgende URL ein: http://**10.0.0.1**/wpad.dat

Variante 2:

Mittels IP des Portalservers

IP-Portalserver: 10.0.0.1

Port: 3128

Bitte aktivieren Sie – je nach Gerät – die Option „Für alle Protokolle diesen Proxy-Server verwenden“.

Diese Einstellungen können an jedem Schulstandort mit installiertem IServ und der **SSID: „WIFI-BYOD“** verwendet werden insofern der Nutzer dort ein freigeschaltetes IServ-Konto hat.

Ist der Nutzer an mehreren Schulen tätig, muss der Proxy nur einmal eingestellt werden und greift dann in allen Schulen gleichermaßen. Damit das funktioniert, müssen jedoch Benutzer und Passwort an allen Schulen gleich sein. Dieses Prozedere trifft auf Sie zu? Dann sprechen Sie bitte die IT-Beauftragten der Schulen dazu an.

Proxyserver erzwingen

Mit der Option Proxy erzwingen in den Eigenschaften eines Gerätes können Sie den kompletten Internetverkehr über den auf dem Portalserver zum Einsatz kommenden Proxyserver umleiten. Damit können dann auch HTTPS-Domains zuverlässig in der Blacklist gesperrt werden. Alle ausgehenden Verbindungen werden in der Firewall des Portalservers gesperrt und nur noch über den Proxy zugelassen.